Red Hat Enterprise Linux 10 Beta

10.0 Beta Release Notes

Release Notes for Red Hat Enterprise Linux 10.0 Beta

Red Hat Enterprise Linux 10 Beta 10.0 Beta Release Notes

Release Notes for Red Hat Enterprise Linux 10.0 Beta

Legal Notice

Abstract

The Release Notes provide high-level coverage of the improvements and additions that have been implemented in Red Hat Enterprise Linux 10.0 Beta 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

RHEL BETA RELEASE

Red Hat provides Red Hat Enterprise Linux Beta access to all subscribed Red Hat accounts. The purpose of Beta access is to:

- Provide an opportunity to customers to test major features and capabilities before the general availability release and provide feedback or report issues.

- Provide Beta product documentation as a preview. Beta product documentation is under development and is subject to substantial change.

Note that Red Hat does not support the usage of RHEL Beta releases in production use cases. For more information, see What does Beta mean in Red Hat Enterprise Linux and can I upgrade a RHEL Beta installation to a General Availability (GA) release?.

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 10.0 BETA

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:

- Disk images, such as AWS or KVM, do not have a separate /**boot** partition.

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

Security

As a Technology Preview, system-wide cryptographic policies (**crypto-policies**), the OpenSSL TLS toolkit, and the OpenSSH suite now work with **post-quantum (PQ) algorithms**.

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

RHEL 10 introduces **Sequoia PGP** tools **sq** and **sqv** that complement the existing GnuPG tools for managing OpenPGP encryption and signatures.

The **OpenSSL** TLS toolkit introduces creation of FIPS-compliant PKCS #12 files, the **pkcs11-provider** for using hardware tokens, and many additional improvements.

RHEL 10 contains the **OpenSSH** suite in version 9.8, which provides many fixes and improvements over OpenSSH 8.7 which was provided in RHEL 9.

The **SELinux** userspace release 3.7 introduces a new option for **audit2allow** providing CIL output mode, Wayland support for the SELinux sandbox, and other improvements.

The **Keylime** agent component is provided in version 0.2.5, which provides support for Initial Device Identity (IDevID) and Initial Attestation Key (IAK) for device identity and uses TLS 1.3 by default.

The **security compliance** offering has evolved substantially compared to RHEL 9 in both the tooling and content. You can still perform all the actions you need to bring your systems close to a compliant state although you might need to use different tools than in previous versions of RHEL.

See New features – Security for more information.

Dynamic programming languages, web and database servers

RHEL 10.0 provides the following dynamic programming languages:

- Python 3.12

- Ruby 3.3

- Node.js 22

- Perl 5.40

- PHP 8.3

RHEL 10.0 includes the following version control systems:

- Git 2.45

- Subversion 1.14

The following web servers are distributed with RHEL 10.0:

- Apache HTTP Server 2.4.62

- nginx 1.26

The following proxy caching servers are available:

- Varnish Cache 7.4

- Squid 6.10

RHEL 10.0 offers the following database servers:

- MariaDB 10.11

- MySQL 8.4

- PostgreSQL 16

- Valkey 7.2

See New features – Dynamic programming languages, web and database servers for more information.

Compilers and development tools
System toolchain
The following system toolchain components are available with RHEL 10.0 Beta:

- GCC 14.2

- glibc 2.39

- Annobin 12.55

- binutils 2.41

Performance tools and debuggers
The following performance tools and debuggers are available with RHEL 10.0 Beta:

- GDB 14.2

- Valgrind 3.23.0

- SystemTap 5.1

- Dyninst 12.3.0

- elfutils 0.191

- libabigail 2.5

Performance monitoring tools
The following performance monitoring tools are available with RHEL 10.0 Beta:

- PCP 6.3.0

- Grafana 10.2.6

Compiler toolsets
The following compiler toolsets are available with RHEL 10.0 Beta:

- LLVM Toolset 18.1.8

- Rust Toolset 1.79.0

- Go Toolset 1.22

For detailed changes, see New featurs – Compilers and development tools .

Identity Management
Key highlights for Identity Management:

- The IdM server functions only partially or not at all. Specifically, you cannot install the **ipa-server-dns** package, and the embedded DNS server cannot be configured using the **-setup-dns** option. Until the necessary updates to **bind-dyndb-ldap** and other impacted components are completed, the integrated DNS feature remains unavailable.

See Known Issues – Identity Management for more information.

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

See New features – The web console for more information.

1.2. 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

1.3. ADDITIONAL RESOURCES

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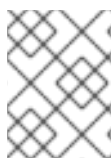
> **NOTE**
>
> Public release notes include links to access the original tracking tickets, but private release notes are not viewable so do not include links.[1]

---

[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. ARCHITECTURES

Red Hat Enterprise Linux 10.0 Beta is distributed with the kernel version 6.11.0, which provides support for the following architectures at the minimum required version (stated in parentheses):

- AMD and Intel 64-bit architectures (x86-64-v3)

- The 64-bit ARM architecture (ARMv8.0-A)

- IBM Power Systems, Little Endian (POWER9)

- 64-bit IBM Z (z14)

Make sure you purchase the appropriate subscription for each architecture.

CHAPTER 3. DISTRIBUTION OF CONTENT IN RHEL 10

3.1. INSTALLATION

Red Hat Enterprise Linux 10 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.

3.2. REPOSITORIES

Red Hat Enterprise Linux 10 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.

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.

3.3. APPLICATION STREAMS

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

Application Streams are available in the following formats:

- RPM format

- Software Collections

- Flatpaks

> **NOTE**
>
> In previous RHEL major versions, some Application Streams were available as modules as an extension to the RPM format. In RHEL 10, Red Hat does not intend to provide any Application Streams that use modularity as the packaging technology and, therefore, no modular content is being distributed with RHEL 10.

Each Application Stream component has a given life cycle, either the same as RHEL 10 or shorter.

RHEL 10 improves the Application Streams experience by providing initial Application Stream versions that can be installed as RPM packages using the **dnf install** command.

> **NOTE**
>
> Certain initial Application Streams in the RPM format have a shorter life cycle than Red Hat Enterprise Linux 10.

Always determine what version of an Application Stream you want to install.

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.

CHAPTER 4. NEW FEATURES AND ENHANCEMENTS

This version adds the following major new features and improvements of some existing features. Some packages might be rebased to a newer upstream version, which provides significant improvements.

4.1. INSTALLER AND IMAGE CREATION

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. 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**. As a consequence, you can create disk images with advanced partitioning layout.

Jira:RHELDOCS-18532[1]

RHEL 10 disk images will have predictable network interface names

The net.ifnames=0 will be removed from kernel arguments, causing all systems to use predictable network interface names. As a consequence, from RHEL 10-beta ongoing, disk images created wih RHEL image builder will now have predictable network interface names. There are no plans for backporting this update to older RHEL versions. As a workaround for older versions, remove the kernel argument after the first boot and reboot the system. See Configuring kernel command-line parameters for more details.

Jira:RHELDOCS-18880[1]

RHEL 10 disk images no longer have a separate /boot partition

RHEL 10 Public Beta disk images, such as AWS images, or KVM images, for example, do not have a separate /**boot** partition. In RHEL images, the /**boot**/ partition removal targets confidential computing.

This change prevents the /**boot** partition from exceeding disk space, which was often the case when /**boot** was on a separate partition. As a result, operational failures are less likely to occur.

Jira:RHELDOCS-18902[1]

New users created in Anaconda are administrators by default

Previously, while creating new users from the installer, the **Add administrative privileges to this user account** option in graphical installation was deselected. Starting RHEL 10, this option is selected by default. As a result, the newly created users will have administrative privileges in the system by default. You can deselect this option to remove the administrative privileges of the new users, if needed.

Jira:RHELDOCS-18425[1]

NVMe over Fabrics devices are now available in the RHEL installation program

You can now add NVMe over Fabrics devices to your RHEL installation to extend the benefits of NVMe storage beyond local devices, enabling the same high-performance, low-latency access over a network. In the RHEL installation program, you can select these devices under the NVMe Fabrics Devices section while adding disks on the Installation Destination screen.

Jira:RHELDOCS-18819[1]

Remote Desktop Protocol (RDP) replaces VNC for graphical remote access

The protocol for graphical remote access has been replaced from VNC to remote desktop protocol (RDP), a more robust, and secure graphical remote access. It offers a reliable and encrypted connection, overcoming the limitations of VNC, which lacked encryption support and enforced password length restrictions.

You can now securely connect to graphical installation sessions. As part of this change, the **inst.vnc**, **inst.vncpassword**, and **inst.vncconnect** kernel boot options have been removed and the new options **inst.rdp**, **inst.rdp.password**, and **inst.rdp.username** have been introduced.

Jira:RHEL-38407

4.2. SECURITY

keylime-agent-rust provided in version 0.2.5

The **keylime-agent-rust** package, which contains the Keylime agent, is provided in version 0.2.5 in RHEL 10. This version offers important enhancements and bug fixes, most importantly the following:

- Added support for Initial Device Identity (IDevID) and Initial Attestation Key (IAK) for device identity. The following configuration options have been added:

  enable_iak_idevid

  > (default: **false**) Enables the use of IDevID and IAK certificates to identify the device.

  iak_idevid_template

  > (default: **detect**) Specifies the template that sets the algorithms to be used for IDevID and IAK (defined in TPM 2.0 Keys for Identity and Attestation, section 7.3.4). The **detect** keyword sets the template according to the algorithms used in the configured certificates.

  iak_idevid_name_alg

  > (default: **sha256**) Specifies the digest algorithm used in IDevID and IAK. Used only if the **iak_idevid_template** option is not set as **detect**.

  iak_idevid_asymmetric_alg

  > (default: **rsa**) Specifies the signing algorithm used in IDevID and IAK. Used only if the **iak_idevid_template** option is not set as **detect**.

  iak_cert

  > (default: **default**) Specifies the path to the file that contains the X509 IAK certificate. The default path is **/var/lib/keylime/iak-cert.crt**.

  idevid_cert

  > (default: **default**) Specifies the path to the file that contains the X509 IDevID certificate. The default path is **/var/lib/keylime/idevid-cert.crt**.

- Configurable IMA and measured boot event log locations are supported by using the new **ima_ml_path** and **measuredboot_ml_path** configuration options.

- Local DNS name, local IP, and configured contact IP are included as part of the Subject Alternative Name of the generated self-signed X509 certificate.

- IPv6 addresses with or without brackets are supported in the **registrar_ip** configuration option.

- Hexadecimal encoded values are supported in the **tpm_ownerpassword** configuration option.

- TLS 1.3 is enabled in connections to the agent.

Jira:RHEL-38409

libreswan provided in version 4.15

The **libreswan** packages are provided in version 4.15 in RHEL 10. This version offers substantial improvements over the previous version 4.12 that was provided in previous releases:

- Removed a dependency on **libxz** through **libsystemd**.

- In IKEv1, default proposals have been set to **aes-sha1** for Encapsulating Security Payload (ESP) and **sha1** for Authentication Header (AH).

- IKEv1 rejects ESP proposals that combine Authenticated Encryption with Associated Data (AEAD) and non-empty INTEG.

- IKEv1 rejects exchange when a connection has no proposals.

- IKEv1 has a more limited default cryptosuite:

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

- Failures of the **libcap-ng** library are no longer fatal.

- TFC padding is set for AEAD algorithms in the **pluto** utility.

Jira:RHEL-52935[1]

New package: rust-sequoia-sq

The Sequoia PGP suite provides a memory-free implementation of the OpenPGP standard for ensuring confidentiality, key management, authentication, and digital signatures. The **sq** command-line tool is a frontend for managing OpenPGP encryption and signatures.

Jira:RHELPLAN-170379[1]

New package: rust-sequoia-sqv

The **sqv** program verifies OpenPGP signatures.

Jira:RHELPLAN-170378[1]

OpenSSH provided in version 9.8

RHEL 10 provides OpenSSH in version 9.8, which introduces many fixes and improvements over OpenSSH 8.7 which was provided in RHEL 9. For the complete list of changes, see the **openssh-9.8p1/ChangeLog** file. The most important changes are as follows:

- A system for restricting forwarding and use of keys that were added to the **ssh-agent** program has been added to **ssh**, **sshd**, **ssh-add**, and **ssh-agent** programs.

- Improvements to the use of the FIDO standard:

  - The **verify-required** certificate option has been added to **ssh-keygen**.

- Fixes to FIDO key handling reduce unnecessary PIN prompts for keys that support intrinsic user verification.

- A check for existing matching credentials in the **ssh-keygen** program prompts the user before overwriting the credential.

- New **EnableEscapeCommandline** option in the **ssh_config** configuration file enables the command line option in the **EscapeChar** menu for interactive sessions.

- New **ChannelTimeout** keyword specifies whether and how quickly the **sshd** daemon should close inactive channels.

- The **ssh-keygen** utility generates Ed25519 keys by default except in FIPS mode, where the default is RSA.

- The **ssh** client performs keystroke timing obfuscation by sending interactive traffic at fixed intervals, every 20 ms by default, when only a small amount of data is being sent. It also sends fake keystrokes for a random interval after the last real keystroke, defined by the **ObscureKeystrokeTiming** keyword.

- DSA keys have been deprecated, and might be removed in a future major release.

- With the new **ChannelTimeout** type, **ssh** and **sshd** close all open channels if all channels lack traffic for a specified interval. This is in addition to the existing per-channel timeouts.

- The **sshd** server blocks client addresses that repeatedly fail authentication, repeatedly connect without ever completing authentication, or that crash the server.

- The **sshd** server penalizes client addresses that do not successfully complete authentication. The penalties are controlled by the new **PerSourcePenalties** keyword in **sshd_config**.

- The **sshd** server is split into a listener binary **sshd** and a per-session binary **sshd-session**. This reduces the listener binary size that does not need to support the SSH protocol. This also removes support for disabling privilege separation and disabling re-execution of **sshd**

- In portable OpenSSH, **sshd** no longer uses **argv[0]** as the PAM service name. You can select the service name at runtime with the new **PAMServiceName** directive in the **sshd_config** file. This defaults to "sshd".

- The **HostkeyAlgorithms** keyword allows **ssh** to disable implicit fallback from certificate host key to plain host keys.

- The components have been hardened in general and work better with the PKCS #11 standard.

Jira:RHEL-42635

Added custom configuration for **pkcs11-provider**

The **pkcs11-provider** allows direct access to hardware tokens by using **pkcs11** URIs from OpenSSL programs. Upon installation, the **pkcs11-provider** is automatically enabled and loads tokens detected by the **pcscd** daemon by using the **p11-kit** driver by default. As a result, you can use tokens available to the system if you provide a key URI by using the **pkcs11** URI specification to an application that supports that format by installing the package without the need to further change OpenSSL configuration. Uninstalling the package also removes the OpenSSL configuration snippet, which prevents errors when OpenSSL parses the configuration files.

Jira:RHEL-29672

File context equivalency set to /var/run = /run in the SELinux policy

The previous **/run = /var/run** file context equivalency is now inverted to **/var/run = /run** and the SELinux policy sources have been updated accordingly. The equivalency has been inverted to match the actual filesystem state and to prevent some userspace tools from reporting an error. This change should not be visible from the user or admin perspective. If you have any custom modules that contain file specification for files in **/var/run**, change them to **/run**.

Jira:RHEL-36094[1]

OpenSSL uses pkcs11-provider for hardware tokens

Because OpenSSL 3.0 deprecated engines and replaced them with providers, RHEL 10 replaces the **openssl-pkcs11** engine with the **pkcs11-provider**. This allows OpenSSL to use hardware tokens in applications such as **apache** HTTPD, **libssh**, **bind**, and other applications that are linked with OpenSSL and use asymmetric private keys stored in an HSM, smartcard or other tokens with a PKCS #11 driver available.

Jira:RHEL-40124

New capability.conf(5) man page

The **capability.conf(5)** man page has been added. It provides descriptions for the **capability.conf** configuration file and the **pam_cap.so** module arguments.

Jira:RHEL-31988

libkcapi provided in version 1.5.0

In RHEL 10.0, the **libkcapi** packages are provided in upstream version 1.5.0. This version provides various bug fixes, optimizations and enhancements, most notably:

- The **sha*** applications have been removed and replaced with a single application called **kcapi-hasher**. Symlinks to **kcapi-hasher** with equivalent names as the original **sha*** applications have been added into the **bin** and **libexec** directories. This change does not cause any known regressions.

- The **sha3sum** command, which prints checksums of files that use **sha3**, has been added.

- The **kcapi_md_sha3_*** wrapper APIs have been added.

Jira:RHEL-50457[1]

Stricter SSH host key permissions have been restored

The necessary host key permissions have been changed from the previous less strict value of **0640** to **0600**, which is also the value used upstream. The **ssh_keys** group, which previously owned all SSH keys, has also been removed. Therefore, the **ssh-keysign** utility uses the SUID bit instead of the SGID bit.

Jira:RHEL-59102[1]

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

CentOS Stream contributors now can participate in the development of the SELinux policy by contributing to the **c10s** branch of the **fedora-selinux/selinux-policy** git repository. These contributions can then be used to improve the SELinux policy of RHEL 10.

Jira:RHEL-33844

p11-kit provided in version 0.25.5

The **p11-kit** packages are provided in version 0.25.5 in RHEL 10. This version provides enhancements and fixes over the previous version, most importantly, the following:

- Support for recursive attributes has been added to the **p11-kit** RPC protocol.

- A function to check run-time version of the library has been added.

- Version information is no longer accessible through macros.

- With the new **--id** option, you can assign an ID to key pairs generated with the **generate-keypair** command or imported with the **import-object** command.

- With the new **--provider** option, you can specify a PKCS #11 module when using **p11-kit** commands.

- Fixed a bug in **p11-kit** where the EdDSA mechanism was not recognized in **generate-keypair**.

- **p11-kit** falls back to the **C_GetFunctionList** function when the **C_GetInterface** function is not supported.

Jira:RHEL-46898[1]

pkeyutil now supports encapsulation and decapsulation

The **pkeyutil** OpenSSL subcommand supports performing encapsulation and decapsulation cryptographic operations. The new post-quantum cryptographic (PQC) algorithm ML-KEM (FIPS 203) permits only encapsulation and decapsulation operations, and you can now use algorithms such as RSASVE and ML-KEM through **pkeyutil**.

Jira:RHEL-54156

GnuTLS can use certificate compression

GnuTLS compresses client and server certificates with the **zlib**, **brotli** or **zstd** compression method according to RFC 8879 if both client and server support and enable it. This method reduces data usage, and should otherwise be unnoticeable to users.

Jira:RHEL-42514[1]

New no-atexit option in OpenSSL

OpenSSL is now built with the **no-atexit** option, so that the **OPENSSL_cleanup** function is no longer registered as an **atexit** handler. Using this option might cause the **valgrind** debugging tool to report one-time memory leaks of the resources allocated on OpenSSL startup.

Jira:RHEL-40408

setools provided in version 4.5.0

The **setools** packages are provided in version 4.5.0 in RHEL 10. This version provides bug fixes and enhancements, most notably the following:

- Graphical results for information flow analysis and domain transition analysis have been added to the **apol**, **sedta**, and **seinfoflow** tools.

- Tooltips and detail popups in **apol** have been added to help cross-referencing query and analyzing results along with context-sensitive help.

Jira:RHEL-29967

RHEL 10 provides NSS in version 3.101

The NSS cryptographic toolkit packages are provided in version 3.101 in RHEL 10, which provides many bug fixes and enhancements. The most notable changes are the following:

- DTLS 1.3 protocol is now supported (RFC 9147).

- PBMAC1 support has been added to PKCS #12 (RFC 9579).

- Experimental support for X25519Kyber768Draft00 hybrid post-quantum key agreement has been added (**draft-tls-westerbaan-xyber768d00**). It will be removed in a future release.

- **lib::pkix** is the default validator in RHEL 10.

- RSA certificates with keys shorter than 2048 bits stop working in SSL servers, in accordance with the system-wide cryptographic policy.

Jira:RHEL-46839

OpenSSL can create FIPS-compliant PKCS #12 files

The OpenSSL secure communication suite has been updated and can now create PKCS #12 files in accordance with the RFC 9579 document.

Jira:RHEL-36659

gnutls provided in version 3.8.7

In RHEL 10.0, the **gnutls** library package is provided in upstream version 3.8.7. This version provides various bug fixes, optimizations and enhancements, most notably:

- Certificate compression in TLS is supported (RFC 8879).

- Optimal Asymmetric Encryption Padding scheme (RSA-OAEP) is supported (RFC 8017).

- API for incremental calculation of SHAKE hashes of arbitrary length across multiple calls has been added.

- RSA encryption and decryption with PKCS #1 v1.5 padding is deprecated and disallowed by default.

- In FIPS mode, **gnutls** now defaults to exporting PKCS #12 files with Password-Based Message Authentication Code 1 (PBMAC1) as defined in RFC 9579. If you need interoperability with systems running in FIPS mode, use PBMAC1 explicitly.

Jira:RHEL-50011[1]

The DEFAULT cryptographic policy uses additional scopes

The **crypto-policies** package now offers additional scopes **@pkcs12**, **@pkcs12-legacy**, **@smime**, and **@smime-legacy**, and uses them in the **DEFAULT** system-wide cryptographic policy. The selection of cryptographic algorithms used for PKCS #12 and S/MIME when network security services (NSS) is the

underlying cryptographic library now follows system-wide cryptographic policies. Therefore, you can more easily select algorithms with higher granularity by using custom policies and subpolicies. The scopes use the following ciphers, hashes, and key exchanges:

```
cipher@pkcs12 = AES-256-CBC AES-128-CBC
cipher@pkcs12-import = 3DES-CBC+ RC2-CBC+
cipher@smime = AES-256-CBC AES-128-CBC 3DES-CBC
cipher@smime-import = RC2-CBC+
hash@{pkcs12,smime} = SHA2-256 SHA2-384 SHA2-512 SHA3-256 SHA3-384 SHA3-512 \
 SHA2-224 SHA3-224
hash@{pkcs12-import,smime} = SHA1+
key_exchange@smime = RSA DH ECDH
```

The **LEGACY** cryptographic policy uses a less strict selection of ciphers, hashes, and key exchanges than the **DEFAULT** policy, whereas the **FUTURE** policy is stricter. As a result, you can customize the algorithms used in NSS for importing and exporting PKCS #12 files and S/MIME encryption and decryption. NSS is currently the only cryptographic library linked to the newly offered scopes.

Jira:RHEL-50655

OpenSSH in FIPS mode generates RSA keys by default

In previous versions, the **ssh-keygen** utility in OpenSSH generated RSA keys by default. In the versions provided with RHEL 10, **ssh-keygen** generates ed25519 keys by default in non-FIPS mode and RSA keys by default in FIPS mode.

Jira:RHEL-37324

NSS creates FIPS-compliant PKCS #12 in FIPS mode

PKCS #12 uses an ad-hoc mechanism for integrity checks. Since the publication of PKCS #12 version 1.1, more rigorous methods of integrity checks have been created in PKCS #5 Version 2.0: the password-based message authentication code 1 (PBMAC1). This update adds PBMAC1 support in PKCS #12 files to Network Security Services (NSS) in accordance with the RFC 9579 document. As a result, NSS can now read any **.p12** file that uses RFC 9579 and can generate RFC-9579-compliant message authentication codes (MAC) when requested by the user. For compatibility, NSS generates old MACs by default when not in FIPS mode. For more information on generating new MACs, see the **pk12util(1)** man page on your system.

Jira:RHEL-39732

clevis provided in version 20

The **clevis** packages are provided in version 20 in RHEL 10. The most notable enhancements and fixes include the following:

- Increased security by fixing potential problems reported by static analyzer tools in the **clevis luks** command, **udisks2** integration, and the Shamir's Secret Sharing (SSS) thresholding scheme.

- Password generation now uses the **jose** utility instead of **pwmake**. This ensures enough entropy for passwords generated during the Clevis binding step.

Jira:RHEL-29279

jose provided in version 14

The **jose** package is provided in version 14 in RHEL 10.   **jose** is a C-language implementation of the Javascript Object Signing and Encryption (JOSE) standards. The most important enhancements and fixes include the following:

- Improved bound checks for the **len** function for the **oct** JWK Type in OpenSSL, as a fix to an error reported by the SAST (Static Application Security Testing) process.

- The protected JSON Web Encryption (JWE) headers no longer contain **zip**.

- **jose** avoids potential denial of service (DoS) attacks by using high decompression chunks.

Jira:RHEL-38084

SELinux userspace provided in version 3.7

RHEL 10 contains the SELinux user-space components in version 3.7. This version introduces enhancements and fixes over the previous version, most importantly, the following:

- New **audit2allow -C** option for the CIL output mode.

- The **sepolgen** utility has been adjusted to parse **refpolicy** modules.

- The **semanage** utility now allows modifying records on **add**.

- The **semanage** utility no longer sorts local **fcontext** definitions.

- The **checkpolicy** program supports the CIDR notation for **nodecon** statements.

- The SELinux sandbox utility now supports the Wayland display protocol.

Jira:RHEL-40233

Rules for additional **libvirt** services added to the SELinux policy

The following SELinux types related to the **libvirt** services have been added to the SELinux policy:

- **virt_dbus_t**

- **virt_hook_unconfined_t**

- **virt_qmf_t**

- **virtinterfaced_t**

- **virtnetworkd_t**

- **virtnodedevd_t**

- **virtnwfilterd_t**

- **virtproxyd_t**

- **virtqemud_t**

- **virtsecretd_t**

- **virtstoraged_t**

- **virtvboxd_t**

- **virtvzd_t**

- **virtxend_t**

Jira:RHEL-46893

SCAP Security Guide is provided in version 0.1.74

The SCAP Security Guide (SSG) packages are provided in upstream version 0.1.74 in RHEL 10-beta.

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

Jira:RHEL-54839

OpenSCAP is provided in version 1.4.0

The **openscap** packages are provided in upstream version 1.4.0 in RHEL 10-beta. Most notable enhancements include:

- You can generate Kickstart files for unattended RHEL installations.

- The **autotailor** tool can process JSON tailoring files that contain multiple profiles.

For additional information, see the OpenSCAP release notes.

Jira:RHEL-53981

4.3. SOFTWARE MANAGEMENT

The repository metadata is now not downloaded by default

Previously, when you downloaded a repository's metadata, the filelists metadata was downloaded by default. The filelists metadata is large and is typically not needed. With this update, this metadata is not downloaded by default, which improves responsiveness and saves disk space. The filelists metadata is also no longer downloaded or updated from repositories and is not loaded into the DNF transaction when you run a **dnf** command. If the **dnf** command requires the filelists metadata or includes a file-related argument, the metadata is loaded automatically.

> **NOTE**
>
> When a package has a filepath dependency that requires filelists metadata to be resolved, the transaction fails with a dependency resolution error and the following hint:
>
> (try to add '--skip-broken' to skip uninstallable packages or '--setopt=optional_metadata_types=filelists' to load additional filelists metadata)

> **NOTE**
>
> If you want to re-enable the default filelist metadata downloading, you can add the **filelists** value to the **optional_metadata_types** option in the **/etc/dnf/dnf.conf** configuration file.

Jira:RHEL-12355[1]

DNF now uses **librpmio** for processing PGP keys

To verify RPM package signatures, RPM uses the **rpm-sequoia** library instead of the previously-used custom PGP parser. With this update, the **librepo** library, which can verify PGP signatures on DNF repositories, now also uses **rpm-sequoia** through the **librpmio** library. As a result, to provide consistent user experience, the **dnf**, **librpm**, and **rpm** components now use the same PGP implementation.

Jira:RHEL-47106

dnf-plugins-core rebased to version 4.7.0

The **dnf-plugins-core** package has been rebased to version 4.7.0 that provides a new **python3-dnf-plugin-pre-transaction-actions** package. This package includes a new **pre-transaction-actions** DNF plugin that allows you to execute a command upon starting an RPM transaction. For more information, see the **dnf-pre-transaction-actions(8)** manual page on your system.

Jira:RHEL-38831

createrepo_c provided in version 1.0.0

RHEL 10 provides the **createrepo_c** package in version 1.0.0. Notable changes over the previous version include:

- Default compression switched from **gz** to **zstd**, which provides smaller metadata that is faster to decompress. Note that the **gz** compression is still supported.

- To save time and disk space, metadata in the SQLite database format is no longer generated by default. Note that you can still create this metadata by using the **--database** switch or the **sqliterepo_c** tool.

- Managing the **group.xml** metadata has been standardized. Previously, this metadata was present twice, as compressed and uncompressed. With this update, the group metadata is present only once as compressed and has the **group** metadata type.

  > **NOTE**
  >
  > The **group.xml** metadata is not compatible with YUM in RHEL 7. If required, you can still create repositories with the old layout by using the **modifyrepo_c** command.

Jira:RHELDOCS-18997[1]

4.4. SHELLS AND COMMAND-LINE TOOLS

openCryptoki rebased to version 3.23.0

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

- **EP11**: Added support for FIPS-session mode

- Various updates are available for protection against RSA timing attacks

Jira:RHEL-24038[1]

polkit rebased to 125

The polkit package is rebased to version 125. Notable enhancements include the following:

- polkit uses the **tmpfiles.d** file to store configuration in the **/etc/polkit-1** directory.

- polkit now supports **syslog-style** log levels and LogControl protocol for dynamic loglevel changing.

The rebase allows the removal of **/etc/polkit-1/<subdirs>** directories and their automatic recreation with appropriate access rules on the next boot. It aligns polkit with the **reset OS to factory settings by deleting /etc** approach. Now, the user does not have to reinstall polkit, if the **etc/polkit-1** directory was deleted.

Additionally, the **polkit.service** unit file now contains a new parameter specified in the call of polkitd daemon, that is, **--log-level=<level>**. By default in RHEL 10, this parameter is set to **--log-level=err**, logging only error messages. If the parameter **--log-level** is omitted, only critical messages are logged.

This change allows users to control how verbose polkit should be in logs and especially in the journal. The enhancement addresses the requirement to log every loaded **.rules** file for debug purposes, preventing the journal from being flooded with unnecessary information.

Jira:RHEL-55287

ksh is rebased to 93u+m/1.0.10

The **KornShell** (ksh) shell is rebased to the 93u+m/1.0.10 version. The notable changes are:

- The **alarm** command, a shell built-in part of ksh, is no longer supported and will be removed. The replacement is the **cron** daemon, a utility for tasks that must run at fixed intervals.

- The ksh shell is now capable of handling more than 32767 simultaneous background jobs, subject to system limitations.

- Fixes a bug that caused an incorrect default exit status for **exit** within a trap action and a race condition occurring on some systems when running an external command with a redirection from a command substitution.

- Various other bug fixes

Jira:RHEL-45981

4.5. INFRASTRUCTURE SERVICES

CUPS broadcast and mDNS are no longer the default configuration for cups-browsed daemon

With this enhancement, the **mDNS** and **CUPS broadcast** service browsing is no longer the default configuration for the **cups-browsed** daemon. As a result, to configure **cups-browsed**, you must add the **BrowsePoll** directive in the **/etc/cups/cups-browsed.conf** file. This file the specifies to the server that the **cups-browsed** daemon polls for printers.

Note: To search on **mDNS** and **CUPS broadcast**, set **BrowseRemoteProtocols dnssd** cups in the **/etc/cups/cups-browsed.conf** file.

Jira:RHELDOCS-17893[1]

tuned-ppd, Valkey, libcpuid and dnsconfd packages are now available

The following packages are included in Red Hat Enterprise Linux:

- **tuned-ppd** : The **tune-ppd** is a replacement of **drop-in power-profiles-daemon** which uses **TuneD** as a backend.

- **Valkey** : Replaces redis and provides the same features.

- **libcpuid** : Enables accurate CPU model identification in **TuneD**.

- **dnsconfd** : A local DNS cache configuration daemon that simplifies setting up DNS caching, split DNS, DNS over TLS, and other DNS features.

Jira:RHELDOCS-18925[1]

GECOS field for user is now changed to Super User

Previously, an application output for the GECOS/description appeared as **root** . Now, the GECOS/description for user **root** in the **/etc/passwd** file has been changed from **root** to **Super User**.

Jira:RHELDOCS-18776[1]

dnsconfd daemon can now be installed

With this enhancement, you can now install the **dnsconfd**, a local DNS cache configuration daemon. The newly configured daemon provides an easy way to set up DNS caching, split DNS, DNS over TLS, and other DNS features.

Jira:RHEL-34791[1]

The Kea DHCP server replaces ISC DHCP

Kea is a new Dynamic Host Configuration Protocol (DHCP) server solution in RHEL. Kea DHCP is an implementation from Internet Systems Consortium (ISC) that includes fully functional DHCPv4, DHCPv6, and Dynamic DNS servers. The Kea DHCP server has the following advantages:

- It is an extensible server solution with module hooks.

- It allows re-configuration through the REST API.

- It has a design that allows separation of data (leases) and execution environment.

Jira:RHEL-9306[1]

intel-lpmd package is now available

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

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

intel-lpmd has the following advantages:

- Improved power efficiency: **intel-lpmd** intelligently distributes workloads between P-cores and E-cores.

- Longer battery life: **intel-lpmd** reduces power consumption during idle periods.

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

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

Start the service:

```
# sudo systemctl start intel_lpmd.service
```
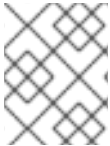
> **NOTE**
>
> By default, you must enable **intel-lpmd** if you are required to meet certain product energy efficiency policies.

Jira:RHELDOCS-18391

4.6. NETWORKING

Enable Duplicate Address Detection for IPv4 in NetworkManager

Generally, assigning the same IP address to multiple systems can cause non-working setups and make it more difficult to debug problems. The Duplicate Address Detection (DAD) mechanism identifies and prevents this issue by ensuring that each IP address within a network is unique. In RHEL 10, the **ipv4.dad-timeout** parameter in NetworkManager has been set to 200ms by default. This enables the DAD functionality for IPv4 addresses on RHEL systems.

Jira:RHEL-1531[1]

4.7. KERNEL

Kernel version in RHEL 10.0 Beta

Red Hat Enterprise Linux 10.0 Beta is distributed with the kernel version 6.11.0.

rh_waived kernel command-line boot parameter is now supported

With this release, the **rh_waived** kernel command-line boot parameter is supported. **rh_waived** is used for enabling waived features in RHEL. The waived features are kernel features considered unmaintained, insecure, rudimentary, or deprecated. These features are disabled by default in RHEL 10. To use waived features, you must enable them manually.

Jira:RHEL-26170[1]

4.8. FILE SYSTEMS AND STORAGE

python-blivet rebased to version 3.10

The **python-blivet** package has been rebased to version 3.10, providing various bug fixes and enhancements. The most notable changes are:

- Removed support for Python 2.

- Support for adding disks to the existing Stratis pool.

- Support for Stratis encryption with Clevis or Tang.

- Support for semi-automatic resizing of the **lvmpv** format to fill underlying block devices.

Jira:RHEL-45175

cryptsetup rebased to version 2.7

The **cryptsetup** package has been rebased to version 2.7. This version provides various bug fixes and enhancements, most notably:

- Improvements for the **libcryptsetup** package to support LUKS encrypted devices in the **kdump** enabled systems.

- Critical fixes for LUKS2 SED OPAL feature.

- Avoids known or already fixed issues with LUSK2 SED OPAL feature.

Jira:RHEL-33395[1]

4.9. HIGH AVAILABILITY AND CLUSTERS

pcs now validates resource parameters when creating or updating a resource

When you create or update a cluster resource, the **pcs** command-line interface now automatically asks the resource agent to validate the parameters you entered. If you specify **--agent-validation**, an invalid parameter yields an error. To maintain backward compatibility, if you do not specify **--agent-validation**, an invalid parameter prints a warning but does not prevent misconfiguration.

Jira:RHEL-35670

New --yes flag to confirm potentially destructive actions

To confirm potentially destructive actions such as destroying a cluster, unblocking quorum, or confirming a node being fenced, the **pcs** command-line interface now supports the **--yes** flag. Previously, you could confirm these actions by using the **--force** flag, which is also used for overriding validation errors. With these two functions combined in a single flag, a user could inadvertently confirm a potentially destructive action when the intention is only to override a validation error. You should now use the **--force** flag to override validation errors, and you should use the **--yes** flag to confirm potentially destructive actions.

Jira:RHEL-36612

New pcs status wait command

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

Jira:RHEL-38491[1]

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

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

- the existence of the resource

- the type of the resource

- the state of the resource

- various information about the members of a collective resource

- on which nodes the resource is running

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

Jira:RHEL-38489[1]

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

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

- Specifying **--output-format=text** displays the configured resource defaults or operation defaults in plain text format, which is the default value for this option.

- Specifying **--output-format=cmd** displays the **pcs resource defaults** or **pcs resource op defaults** commands created from the current cluster defaults configuration. You can use these commands to re-create configured resource defaults or resource operation defaults on a different system.

- Specifying **--output-format=json** displays the configured resource defaults or resource operation defaults in JSON format, which is suitable for machine parsing.

Jira:RHEL-38487[1]

pcsd Web UI now available as a RHEL web console add-on

The **pcsd** Web UI is now available as the HA Cluster Management RHEL web console add-on when the **cockpit-ha-cluster** package is installed. It is no longer operated as a standalone interface.

Jira:RHEL-23048

RHEL 10 provides Pacemaker version 2.1.8

Pacemaker has been upgraded to version 2.1.8, which provides multiple bug fixes and enhancements. Notable changes include:

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

- The CIB manager no longer increases in size indefinitely with each request from an asynchronous client. Previously, when the CIB manager received a request from an asynchronous client, it leaked a small amount of memory. This caused the CIB manager process gradually to grow in size. With this upgrade, the relevant memory is freed for asynchronous clients and the CIB manager process no longer grows in size indefinitely.

Jira:RHEL-38543

Support for new Ha Cluster Management features

For RHEL 10, the **pcsd** Web UI is now available as a RHEL web console add-on as the HA Cluster Management application. It is no longer operated as a standalone interface. The HA Cluster Management application now supports the following features:

- When you set the **placement-strategy** cluster property to **default**, the HA Cluster Management application displays a warning near the utilization attributes for nodes and resources. This warning notes that the utilization has no effect due to **placement-strategy** configuration.

- The HA Cluster Management application supports dark mode, which you can set through the user menu in the masthead.

Jira:RHEL-38493[1], Jira:RHEL-38496

4.10. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS

Python 3.12 in RHEL 10

Python 3.12 is the default Python implementation in RHEL 10. Python 3.12 is distributed as a non-modular **python3** RPM package in the BaseOS repository and is usually installed by default. Python 3.12 will be supported for the whole life cycle of RHEL 10.

Additional versions of Python 3 will be distributed as RPM packages with a shorter life cycle through the AppStream repository and will be installable in parallel. The **python** command (**/usr/bin/python**), as well as other Python-related commands, such as **pip**, are available in the unversioned form and point to the default Python 3.12 version.

Notable enhancements compared to the previously released Python 3.11 include:

- Python introduces a new **type** statement and new type parameter syntax for generic classes and functions.

- Formatted string literal (f-strings) have been formalized in the grammar and can now be integrated into the parser directly.

- Python now provides a unique per-interpreter global interpreter lock (GIL).

- You can now use the buffer protocol from Python code.

- Dictionary, list, and set comprehensions in **CPython** are now inlined. This significantly increases the speed of a comprehension execution.

- **CPython** now supports the Linux **perf** profiler.

- **CPython** now provides stack overflow protection on supported platforms.

- Python 3.12 is compiled with GCC's **-O3** optimization flag, which has been used by default in upstream. As a result, you can observe increased performance of your Python applications and the interpreter.

To install packages from the Python 3.12 stack, you can use, for example, the following commands:

```
# dnf install python3
# dnf install python3-pip
```

To run the interpreter, you can use, for example, the following commands:

```
$ python
$ python3
$ python3 -m pip --help
```

Jira:RHELDOCS-18402[1], Jira:RHEL-45315

RHEL 10 introduces Perl 5.40

RHEL 10 includes Perl 5.40, which provides various enhancements over the previously available version 5.32.

- Core enhancements:

  - Perl now supports Unicode 15.0.

  - You can now use a new **-g** command-line option, which is an alias for the umask option **-0777**.

  - The **-M** command-line option now accepts a space.

  - A new **builtin** module now provides documentation for new always-present functions.

  - A new **try**/**catch** feature has been added.

  - Deprecation warnings now have specific subcategories to provide finer-grained control. Note that you can still disable all deprecation warnings in a single statement.

  - The **@INC** hooks have been enhanced, including the **$INC** variable and the new **INCDIR** method.

  - Forbidden control flow out of the **defer** and **finally** modules is now detected at compile-time.

  - The use of **(?{ ... })** and **(??{ ... })** in a pattern now disables various optimisations globally in that pattern.

  - The limit for the **REG_INF** regex engine quantifier has been increased from 65,536 to 2,147,483,647.

  - A new regexp variable **${^LAST_SUCCESSFUL_PATTERN}** allows access to the last successful pattern that matched in the current scope.

  - A new **__CLASS__** keyword has been introduced.

  - Perl now supports a new **^^** logical XOR operator.

- Incompatible changes:

  - A physically empty **sort** function now triggers a compile-time error.

  - The **readline()** function no longer clears the stream error and EOF flags.

  - **INIT** blocks no longer run after an **exit()** function inside a **BEGIN** block.

  - Calling the **import** method on an unknown package now produces a warning.

  - The **return** function no longer allows an indirect object.

- Changes in errors and warnings can now cause failures in tests.

- Deprecations:

    - The use of the **'** character as a package name separator is deprecated.

    - The **switch** feature and the smartmatch operator `~~` are deprecated.

    - Using the **goto** function to jump from an outer scope into an inner scope is deprecated.

- Internal changes:

    - Multiple deprecated C functions have been removed.

    - Internal C API functions are now hidden with the **__attribute__((hidden))** attribute on the platforms that support it. This means they are no longer callable from XS modules on those platforms.

- Modules:

    - The **Term::Table** and **Test2::Suite** modules have been added to Perl Core.

    - Most modules have been updated.

For more information, see the **perl5340delta**, **perl5360delta**, **perl5380delta**, and **perldelta** man pages.

Jira:RHELDOCS-18869[1]

RHEL 10 provides **Node.js 22**

RHEL 10 is distributed with **Node.js 22**. This version provides numerous new features, bug fixes, security fixes, and performance improvements over previously available **Node.js 20**.

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.

Jira:RHEL-35992

RHEL 10 introduces MySQL 8.4

RHEL 10 is distributed with MySQL 8.4. Notable changes over the previously available version 8.0 include:

- The deprecated **mysql_native_password** authentication plug-in is no longer enabled by default.

- When upgrading to MySQL 8.4, user accounts or roles that have the **BINLOG_ADMIN** privilege are automatically granted the **TRANSACTION_GTID_TAG** privilege.

- When you install MySQL 8.4, the **mysql_upgrade_history** file is created or updated in the server's data directory. The file is in JSON format and includes information about the version installed, date and time of installation, and whether the release was part of a Long-Term Support (LTS series) or an Innovation series.

- The use of the **%** and _ characters as wildcards in database grants has been deprecated, and the wildcard functionality will be removed in a future MySQL release. These characters will be treated as literals. They are already treated as literals when the **partial_revokes** server system variable is set to **ON**.

- The treatment of the **%** character by the server as a synonym for localhost when checking privileges has been deprecated.

- The deprecated **--ssl** and **--admin-ssl** server options and **have_ssl** and **have_openssl** server system variables have been removed. Use the **--tls-version** and **--admin-tls-version** server system variables instead.

- The deprecated **default_authentication_plugin** system variable has been removed. Use the **authentication_policy** server system variable instead.

- The deprecated **SET_USER_ID** privilege has been removed. Instead, you can use the **SET_ANY_DEFINER** privilege for definer object creation and the **ALLOW_NONEXISTENT_DEFINER** privileges for orphan object protection.

- The deprecated **mysql_upgrade** utility has been removed.

For more information, see the upstream MySQL documentation.

Jira:RHEL-36050

RHEL 10 provides PostgreSQL 16 with the pgvector extension

RHEL 10 is distributed with PostgreSQL 16. In addition to the **pgaudit**, **pg_repack**, and **decoderbufs** extensions, the Postgresql stack now provides the **pgvector** extension. With the **pgvector** extension, you can store and query high-dimensional vector embeddings directly within PostgreSQL databases and perform a vector similarity search. Vector embeddings are numerical representations of data that are often used in machine learning and AI applications to capture the semantic meaning of text, images, or other data types.

Jira:RHEL-35993[1]

4.11. COMPILERS AND DEVELOPMENT TOOLS

RHEL 10 introduces GCC 14.2

RHEL 10 is distributed with the GNU Compiler Collection (GCC) version 14.2.

Notable changes since GCC 13 include:

- Optimization and diagnostic improvements

- A new **-fhardened** umbrella option, which enables a set of hardening flags

- A new **-fharden-control-flow-redundancy** option to detect attacks that transfer control into the middle of functions

- A new **strub** type attribute to control stack scrubbing properties of functions and variables

- A new **-finline-stringops** option to force inline expansion of certain **mem*** functions

- Support for new OpenMP 5.1, 5.2, and 6.0 features

- Several new C23 features

- Multiple new C++23 and C++26 features

- Several resolved C++ defect reports

- New and improved experimental support for C++20, C++23, and C++26 in the C++ library

- Support for new CPUs in the 64-bit ARM architecture

- Multiple new instruction set architecture (ISA) extensions in the 64-bit Intel architecture, for example: AVX10.1, AVX-VNNI-INT16, SHA512, and SM4

- New warnings in the GCC's static analyzer

- Certain warnings changed to errors; for details, see Porting to GCC 14

- Various bug fixes

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

Jira:RHEL-45041

GCC 14 defaults to x86-64-v3

GCC 14 in RHEL 10 defaults to the x86-64-v3 microarchitecture level. This level enables certain capabilities by default, such as the AVX and AVX2 instruction sets and the fused multiply-add (FMA) instruction set. See the related article for more details.

Jira:RHEL-33254

GCC defaults to using the **IEEE128** floating point format on IBM Power Systems

In RHEL10, GCC uses the **IEEE128** floating point format by default for all long double floating point numbers on IBM Power Systems instead of the earlier software-only **IBM-DOUBLE-DOUBLE** code. As a result, you can notice performance improvements in C or C++ code that performs computations by using long double floating point numbers.

Note that this 128-bit long double floating point ABI is incompatible with the floating point ABI used in RHEL 8 and earlier versions. Support for hardware instructions to perform **IEEE128** operations is available since IBM POWER9.

Jira:RHEL-24760[1]

RHEL 10 includes **annobin** version 12.55

RHEL 10 is distributed with **annobin** version 12.55. Notable changes over the previously available version 12.32 include:

- Updated tools to build and work with newer versions of the GCC, Clang, LLVM, and Go compilers

- Recording and testing for the use of the GCC command-line options **-Wimplicit-int** and **-Wimplicit-function-declaration**

- Improved support for LLVM

- New tests

- A new check to identify if the deprecated OpenSSL Engine code is used

- Various bug fixes

Jira:RHEL-526[1]

RHEL 10 includes **binutils** version 2.41

RHEL 10 is distributed with **binutils** version 2.41. Notable changes over the previously available version 2.40 include:

- **binutils** tools support architecture extensions in the 64-bit Intel and ARM architectures.

- The linker now accepts the **--remap-inputs <PATTERN>=<FILE>** command-line option to replace any input file that matches **<PATTERN>** with **<FILE>**. In addition, you can use the **--remap-inputs-file=<FILE>** option to specify a file containing any number of these remapping directives.

- For ELF targets, you can use the linker command-line option **--print-map-locals** to include local symbols in a linker map.

- For most ELF-based targets, you can use the **--enable-linker-version** option to insert the version of the linker as a string into the **.comment** section.

- The linker script syntax has a new command for output sections, **ASCIZ "<string>"**, which inserts a zero-terminated string at the current location.

- You can use the new **-z nosectionheader** linker command-line option to omit ELF section header.

Jira:RHELDOCS-18761[1]

The **ld** linker of **binutils** supports the **--section-ordering-file** option

You can now use the new **--section-ordering-file** command-line option with **ld.bfd**, the default system linker, to group sections of code or data that can benefit from being in proximity to each other.

This feature improves performance of programs by reducing cache misses. You can use profiling tools to analyze use of your program's code over time, and then improve code grouping in the executable image. As a result, you have more control over the layout of your programs in memory.

The **--section-ordering-file** option also enhances compatibility with the **gold** and **lld** linkers, which already provide this feature.

For details, see the blog post A practical guide to linker section ordering .

glibc now supports dynamic linking of Intel APX-enabled functions

An incompatible dynamic linker trampoline was identified as a potential source of incompatibilities for Intel Advanced Performance Extensions (APX) applications. As a workaround, it was possible to use the **BIND_NOW** executable or use only the standard calling convention. With this update, the dynamic linker of **glibc** preserves APX-related registers.
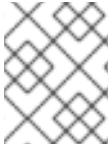
> **NOTE**
>
> Because of this change, additional space is needed beyond the top of the stack. Users who strictly limit this space might need to adjust or evaluate the stack limits.

RHEL 10 provides glibc version 2.39

RHEL 10 introduces GNU C Library (**glibc**) version 2.39.

Optimization of AMD Zen 3 and Zen 4 performance in glibc

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

RHEL 10 provides GDB version 14.2

GDB has been updated to version 14.2. The following paragraphs list notable changes since GDB 12.1.

General:

- The **info breakpoints** command now displays enabled breakpoint locations of disabled breakpoints as in the **y-** state.

- Added support for debug sections compressed with Zstandard (**ELFCOMPRESS_ZSTD**) for ELF.

- The Text User Interface (TUI) no longer styles the source and assembly code highlighted by the current position indicator by default. To re-enable styling, use the new command **set style tui-current-position**.

- A new **$_inferior_thread_count** convenience variable contains the number of live threads in the current inferior.

- For breakpoints with multiple code locations, GDB now prints the code location using the **<breakpoint_number>.<location_number>** syntax.

- When a breakpoint is hit, GDB now sets the **$_hit_bpnum** and **$_hit_locno** convenience variables to the hit breakpoint number and code location number. You can now disable the last hit breakpoint by using the **disable $_hit_bpnum** command, or disable only the specific breakpoint code location by using the **disable $_hit_bpnum.$_hit_locno** command.

- Added support for the **NO_COLOR** environment variable.

- Added support for integer types larger than 64 bits.

- You can use new commands for multi-target feature configuration to configure remote target feature sets (see the **set remote <name>-packet** and **show remote <name>-packet** in Commands).

- Added support for the Debugger Adapter Protocol.

- You can now use the new **inferior** keyword to make breakpoints inferior-specific (see **break** or **watch** in Commands).

- You can now use the new **$_shell()** convenience function to execute a shell command during expression evaluation.

Changes to existing commands:

- **break**, **watch**

  - Using the **thread** or **task** keywords multiple times with the **break** and **watch** commands now results in an error instead of using the thread or task ID of the last instance of the keyword.

  - Using more than one of the **thread**, **task**, and **inferior** keywords in the same **break** or **watch** command is now invalid.

- **printf**, **dprintf**

  - The **printf** and **dprintf** commands now accept the **%V** output format, which formats an expression the same way as the **print** command. You can also modify the output format by using additional print options in brackets **[…]** following the command, for example: **printf "%V[-array-indexes on]", <array>**.

- **list**

  - You can now use the **.** argument to print the location around the point of execution in the current frame, or around the beginning of the **main()** function if the inferior has not started yet.

  - Attempting to list more source lines in a file than are available now issues a warning, referring the user to the **.** argument.

- **document user-defined**

  - It is now possible to document user-defined aliases.

New commands:

- **set print nibbles [on|off]** (default: **off**), **show print nibbles** – controls whether the **print/t** command displays binary values in groups of four bits (nibbles).

- **set debug infcall [on|off]** (default: **off**), **show debug infcall** – prints additional debug messages about inferior function calls.

- **set debug solib [on|off]** (default: **off**), **show debug solib** – prints additional debug messages about shared library handling.

- **set print characters <LIMIT>**, **show print characters**, **print -characters <LIMIT>** - controls how many characters of a string are printed.

- **set debug breakpoint [on|off]** (default: **off**), **show debug breakpoint** - prints additional debug messages about breakpoint insertion and removal.

- **maintenance print record-instruction [N]** - prints the recorded information for a given instruction.

- **maintenance info frame-unwinders** - lists the frame unwinders currently in effect in the order of priority (highest first).

- **maintenance wait-for-index-cache** - waits until all pending writes to the index cache are completed.

- **info main** - prints information on the main symbol to identify an entry point into the program.

- **set tui mouse-events [on|off]** (default: **on**), **show tui mouse-events** - controls whether mouse click events are sent to the TUI and Python extensions (when **on**), or the terminal (when **off**).

Machine Interface (MI) changes:

- MI version 1 has been removed.

- MI now reports **no-history** when reverse execution history is exhausted.

- The **thread** and **task** breakpoint fields are no longer reported twice in the output of the **-break-insert** command.

- Thread-specific breakpoints can no longer be created on non-existent thread IDs.

- The **--simple-values** argument to the **-stack-list-arguments**, **-stack-list-locals**, **-stack-list-variables**, and **-var-list-children** commands now considers reference types as simple if the target is simple.

- The **-break-insert** command now accepts a new **-g thread-group-id** option to create inferior-specific breakpoints.

- Breakpoint-created notifications and the output of the **-break-insert** command can now include an optional **inferior** field for the main breakpoint and each breakpoint location.

- The async record stating the **breakpoint-hit** stopped reason now contains an optional field **locno** giving the code location number in case of a multi-location breakpoint.

Changes in the GDB Python API:

- Events

  - A new **gdb.ThreadExitedEvent** event.

  - A new **gdb.executable_changed** event registry, which emits the **ExecutableChangedEvent** objects that have **progspace** and **reload** attributes.

  - New **gdb.events.new_progspace** and **gdb.events.free_progspace** event registries, which emit the **NewProgspaceEvent** and **FreeProgspaceEvent** event types. Both of these event types have a single attribute **progspace** to specify the **gdb.Progspace** program space that is being added to or removed from GDB.

- The **gdb.unwinder.Unwinder** class

  - The **name** attribute is now read-only.

  - The name argument of the **__init__** function must be of the **str** type, otherwise a **TypeError** is raised.

  - The **enabled** attribute now accepts only the **bool** type.

- The **gdb.PendingFrame** class

  - New methods: **name**, **is_valid**, **pc**, **language**, **find_sal**, **block**, and **function**, which mirror similar methods of the **gdb.Frame** class.

  - The **frame-id** argument of the **create_unwind_info** function can now be either an integer or a **gdb.Value** object for the **pc**, **sp**, and **special** attributes.

- A new **gdb.unwinder.FrameId** class, which can be passed to the **gdb.PendingFrame.create_unwind_info** function.

- The **gdb.disassembler.DisassemblerResult** class can no longer be sub-classed.

- The **gdb.disassembler** module now includes styling support.

- A new **gdb.execute_mi(COMMAND, [ARG]...)** function, which invokes a GDB/MI command and returns result as a Python dictionary.

- A new **gdb.block_signals()** function, which returns a context manager that blocks any signals that GDB needs to handle.

- A new **gdb.Thread** subclass of the **threading.Thread** class, which calls the **gdb.block_signals** function in its **start** method.

- The **gdb.parse_and_eval** function has a new **global_context** parameter to restrict parsing on global symbols.

- The **gdb.Inferior** class

  - A new **arguments** attribute, which holds the command-line arguments to the inferior, if known.

  - A new **main_name** attribute, which holds the name of the inferior's **main** function, if known.

  - New **clear_env**, **set_env**, and **unset_env** methods, which can modify the inferior's environment before it is started.

- The **gdb.Value** class

  - A new **assign** method to assign a value of an object.

  - A new **to_array** method to convert an array-like value to an array.

- The **gdb.Progspace** class

  - A new **objfile_for_address** method, which returns the **gdb.Objfile** object that covers a given address (if exists).

- A new **symbol_file** attribute holding the **gdb.Objfile** object that corresponds to the **Progspace.filename** variable (or **None** if the filename is **None**).

- A new **executable_filename** attribute, which holds the string with a filename that is set by the **exec-file** or **file** commands, or **None** if no executable file is set.

- The **gdb.Breakpoint** class

  - A new **inferior** attribute, which contains the inferior ID (an integer) for breakpoints that are inferior-specific, or **None** if no such breakpoints are set.

- The **gdb.Type** class

  - New **is_array_like** and **is_string_like** methods, which reflect whether a type might be array- or string-like regardless of the type's actual type code.

- A new **gdb.ValuePrinter** class, which can be used as the base class for the result of applying a pretty-printer.

- A newly implemented **gdb.LazyString.__str__** method.

- The **gdb.Frame** class

  - A new **static_link** method, which returns the outer frame of a nested function frame.

  - A new **gdb.Frame.language** method that returns the name of the frame's language.

- The **gdb.Command** class

  - GDB now reformats the doc string for the **gdb.Command** class and the **gdb.Parameter** sub-classes to remove unnecessary leading whitespace from each line before using the string as the help output.

- The **gdb.Objfile** class

  - A new **is_file** attribute.

- A new **gdb.format_address(ADDRESS, PROGSPACE, ARCHITECTURE)** function, which uses the same format as when printing address, symbol, and offset information from the disassembler.

- A new **gdb.current_language** function, which returns the name of the current language.

- A new Python API for wrapping GDB's disassembler, including **gdb.disassembler.register_disassembler(DISASSEMBLER, ARCH)**, **gdb.disassembler.Disassembler**, **gdb.disassembler.DisassembleInfo**, **gdb.disassembler.builtin_disassemble(INFO, MEMORY_SOURCE)**, and **gdb.disassembler.DisassemblerResult**.

- A new **gdb.print_options** function, which returns a dictionary of the prevailing print options, in the form accepted by the **gdb.Value.format_string** function.

- The **gdb.Value.format_string** function

  - **gdb.Value.format_string** now uses the format provided by the **print** command if it is called during a **print** or other similar operation.

  - **gdb.Value.format_string** now accepts the **summary** keyword.

- A new **gdb.BreakpointLocation** Python type.

- The **gdb.register_window_type** method now restricts the set of acceptable window names.

Architecture-specific changes:

- AMD and Intel 64-bit architectures

  - Added support for disassembler styling using the **libopcodes** library, which is now used by default. You can modify how the disassembler output is styled by using the **set style disassembler *** commands. To use the Python Pygments styling instead, use the new **maintenance set libopcodes-styling off** command.

- The 64-bit ARM architecture

  - Added support for dumping memory tag data for the Memory Tagging Extension (MTE).

  - Added support for the Scalable Matrix Extension 1 and 2 (SME/SME2). Some features are still considered experimental or alpha, for example, manual function calls with ZA state or tracking Scalable Vector Graphics (SVG) changes based on DWARF.

  - Added support for Thread Local Storage (TLS) variables.

  - Added support for hardware watchpoints.

- The 64-bit IBM Z architecture

  - Record and replay support for the new **arch14** instructions on IBM Z targets, except for the specialized-function-assist instruction **NNPA**.

- IBM Power Systems, Little Endian

  - Added base enablement support for POWER11.

For changes since the RHEL 9 system version of GDB 10.2, see the release notes for the GCC Toolset 12 version of GDB 11.2 and the GCC Toolset 13 version of GDB 12.1 .

Jira:RHEL-33256, Jira:RHEL-24764, Jira:RHEL-39324

RHEL 10 provides **elfutils** version 0.191

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

- Changes in the **libdw** library:

  - The **dwarf_addrdie** function now supports binaries lacking a **debug_aranges** section.

  - Support for DWARF package files has been improved.

  - A new **dwarf_cu_dwp_section_info** function has been added.

- Caching eviction logic in the **debuginfod** server has been enhanced to improve retention of small, frequent, or slow files, such as **vdso.debug**.

- The **eu-srcfiles** utility can now fetch the source files of a DWARF/ELF file and place them into a **zip** archive.

Jira:RHEL-29197

RHEL 10 provides **SystemTap** version 5.1

RHEL 10 includes the **SystemTap** tracing and probing tool version 5.1. Notable changes since version 5.0 include:

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

- Improved support for probing processes running in containers, identified by host PID.

- New probes for userspace hardware breakpoints and watchpoints.

- Support for the **--remote** operation of **--runtime=bpf** mode.

- Improved robustness of kernel-user transport.

Jira:RHEL-29529

RHEL 10 provides **Valgrind** version 3.23.0

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

- The **--track-fds=yes** option now warns against double closing of file descriptors, generates suppressible errors, and supports XML output.

- The **--show-error-list=no|yes** option now accepts a new value, **all**, to also print the suppressed errors.

- On the 64-bit IBM Z architecture, **Valgrind** now supports neural network processing assist (NNPA) facility vector instructions: **VCNF**, **VCLFNH**, **VCFN**, **VCLFNL**, **VCRNF**, and **NNPA** (z16/arch14).

- On the 64-bit ARM architecture, **Valgrind** now supports **dotprod** instructions (**sdot/udot**).

- On the AMD and Intel 64-bit architectures, **Valgrind** now provides more accurate instruction support for the x86_64-v3 microarchitecture.

- **Valgrind** now provides wrappers for the **wcpncpy**, **memccpy**, **strlcat**, and **strlcpy** functions that can detect memory overlap.

- **Valgrind** now supports the following Linux syscalls: **mlock2**, **fchmodat2**, and **pidfd_getfd**.

Jira:RHEL-29535

RHEL 10 introduces **Dyninst** version 12.3.0

RHEL 10 is distributed with the **Dyninst** library version 12.3.0.

Jira:RHEL-49597[1]

RHEL 10 provides **libabigail** version 2.5

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

- Improved suppression specification for strict conversions of flexible array data members.

- Added support for pointer-to-member types in C++ binaries.

- Improved **weak** mode of the **abicompat** tool.

- A new **abidb** tool to manage the ABI of operating systems.

- Numerous bug fixes.

Jira:RHEL-30014

RHEL 10 Beta introduces LLVM Toolset 18.1.8

RHEL 10 Beta is distributed with the LLVM Toolset version 18.1.8.

Notable LLVM updates:

- The constant expression variants of the following instructions have been removed: **and**, **or**, **lshr**, **ashr**, **zext**, **sext**, **fptrunc**, **fpext**, **fptoui**, **fptosi**, **uitofp**, **sitofp**.

- The **llvm.exp10** intrinsic has been added.

- The **code_model** attribute for global variables has been added.

- The backend for the AArch64, AMDGPU, PowerPC, RISC-V, SystemZ and x86 architectures has been improved.

- LLVM tools have been improved.

Notable Clang enhancements:

- C++20 feature support:

  - Clang no longer performs One Definition Rule (ODR) checks for declarations in the global module fragment. To enable more strict behavior, use the **-Xclang -fno-skip-odr-check-in-gmf** option.

- C++23 feature support:

  - A new diagnostic flag **-Wc++23-lambda-attributes** has been added to warn about the use of attributes on lambdas.

- C++2c feature support:

  - Clang now allows using the _ character as a placeholder variable name multiple times in the same scope.

  - Attributes now expect unevaluated strings in attribute parameters that are string literals.

  - The deprecated arithmetic conversion on enumerations from C++26 has been removed.

  - The specification of template parameter initialization has been improved.

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

ABI changes in Clang:

- Following the SystemV ABI for x86_64, the **__int128** arguments are no longer split between a register and a stack slot.

- For more information, see the list of ABI changes in Clang .

Notable backwards incompatible changes:

- A bug fix in the reversed argument order for templated operators breaks code in C++20 that was previously accepted in C++17.

- The **GCC_INSTALL_PREFIX** CMake variable (which sets the default **--gcc-toolchain=**) is deprecated and will be removed. Specify the **--gcc-install-dir=** or **--gcc-triple=** option in a configuration file instead.

- The default extension name for precompiled headers (PCH) generation (**-c -xc-header** and **-c -xc++-header**) is now **.pch** instead of **.gch**.

- When **-include a.h** probes the **a.h.gch** file, the include now ignores **a.h.gch** if it is not a Clang PCH file or a directory containing any Clang PCH file.

- A bug that caused **__has_cpp_attribute** and **__has_c_attribute** to return incorrect values for certain C++-11-style attributes has been fixed.

- A bug in finding a matching **operator!=** while adding a reversed **operator==** has been fixed.

- The name mangling rules for function templates have been changed to accept that functions can be overloaded on their template parameter lists or requires-clauses.

- The **-Wenum-constexpr-conversion** warning is now enabled by default on system headers and macros. It will be turned into a hard (non-downgradable) error in the next Clang release.

- A path to the imported modules for C++20 named modules can no longer be hardcoded. You must specify all the dependent modules from the command line.

- It is no longer possible to import modules by using **import <module>**; Clang uses explicitly-built modules.

- For more details, see the list of potentially breaking changes.

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

LVM Toolset is a rolling Application Stream, and only the latest version is supported.

Jira:RHEL-28056

RHEL 10 Beta includes Rust Toolset version 1.79.0

RHEL 10 Beta is distributed with the Rust Toolset version 1.79.0. Notable enhancements since the previously available version 1.75.0 include:

- A new **offset_of!** macro

- Support for C-string literals

- Support for inline **const** expressions

- Support for bounds in associated type position

- Improved automatic temporary lifetime extension

- Debug assertions for **unsafe** preconditions

Rust Toolset is a rolling Application Stream, and only the latest version is supported.

Jira:RHEL-30071

RHEL 10 Beta provides Go Toolset version 1.22

RHEL 10 Beta introduces the Go Toolset version 1.22. Notable enhancements since the previously available version 1.21 include:

- Variables in for loops are now created per iteration, preventing accidental sharing bugs. Additionally, for loops can now range over integers.

- Commands in workspaces can now use a vendor directory for the dependencies of the workspace.

- The **go get** command no longer supports the legacy **GOPATH** mode. This change does not affect the **go build** and **go test** commands.

- The **vet** tool has been updated to match the new behavior of the for loops.

- CPU performance has been improved by keeping type-based garbage collection metadata nearer to each heap object.

- Go now provides improved inlining optimizations and better profile-guided optimization support for higher performance.

- A new **math/rand/v2** package is available.

- Go now provides enhanced HTTP routing patterns with support for methods and wildcards.

For more information, see the Go upstream release notes.

Go Toolset is a rolling Application Stream, and only the latest version is supported.

Jira:RHEL-46971

RHEL 10 includes PCP version 6.3.0

RHEL 10 is distributed with Performance Co-Pilot (PCP) version 6.3.0. Notable changes over the previously available version 6.2.0 include:

New tools and agents

- **pcp2openmetrics**: a new tool to push PCP metrics in Open Metrics format to remote end points

- **pcp-geolocate**: a new tool to report latitude and longitude metric labels

- **pmcheck**: a new tool to interrogate and control PCP components

- **pmdauwsgi**: a new PCP agent that exports instrumentation from uWSGI servers

Enhanced tools

- **pmdalinux**: added new kernel metrics (hugepages, filesystems, TCP, softnet, virtual machine balloon)

- **pmdalibvirt**: added support for metric labels, added new balloon, vCPU, and domain info metrics

- **pmdabpf**: improved eBPF networking metrics for use with the **pcp-atop** utility

Jira:RHELDOCS-18787[1]

RHEL 10 provides **Grafana** version 10.2.6

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

Notable enhancements include:

- Support for zooming in on the y axis of time series and candlestick visualizations by holding shift while clicking and dragging.

- Streamlined data source selection when creating a dashboard.

- Updated User Interface, including updates to navigation and the command palette.

- Various improvements to transformations, including the new unary operation mode for the **Add field from calculation** transformation.

- Various improvements to dashboards and data visualizations, including a redesigned empty dashboard and dashboard panel.

- New geomap and canvas panels.

Other changes:

- Various improvements to users, access, authentication, authorization, and security.

- Alerting improvements along with new alerting features.

- Public dashboards now available.

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

Jira:RHEL-35761

Grafana, PCP, and **grafana-pcp** now use **Valkey** to store data

In RHEL 10, the **Valkey** key-value store replaces **Redis**. As a result, **Grafana**, PCP, and the **grafana-pcp** plug-in now use **Valkey** to store data instead of **Redis**. The **PCP Redis** data source in the **grafana-pcp** plug-in is now named **PCP Valkey**.

Jira:RHEL-45646

zlib-ng-compat replaces **zlib** in RHEL 10

The new **zlib-ng-compat** package provides a general-purpose lossless data compression library that is used by many different programs. This implementation provides various benefits over **zlib** distributed in RHEL 9. For example, **zlib-ng-compat** supports hardware acceleration when available and enhances compression efficiency and performance. **zlib-ng-compat** is built in API and ABI compatible mode to ensure a smooth transition from **zlib**.

Jira:RHEL-24058[1]

SWIG 4.2.1 available in the CRB repository

The Simplified Wrapper and Interface Generator (SWIG) version 4.2.1 is now available in the CodeReady Linux Builder (CRB) repository. Notable changes include:

- Python Standard Template Library (STL) container wrappers now use the Python Iterator Protocol.

- SWIG now supports:

  - Python stable Application Binary Interface (ABI)

  - Python 3.12 and Python 3.13

  - Ruby 3.2 and Ruby 3.3

  - Tcl 9.0

  - PHP 8; support for PHP 7 has been removed.

- Support for the C++14 auto variable without trailing return type for the C++11 auto variable has been added.

- Constructors, destructors, and assignment operators have been fixed, including implicit, default, and deleted, and related non-assignable variable wrappers.

- A new Javascript generator targeting Node.js binary stable ABI Node-API is now available.

- Multiple deprecated features have been removed.

Note that packages included in the CodeReady Linux Builder repository are unsupported.

Jira:RHELDOCS-19059[1]

Red Hat build of OpenJDK 21 is the default Java implementation in RHEL 10

The default RHEL 10 Java implementation is OpenJDK 21. Use the **java-21-openjdk** packages, which provide the OpenJDK 21 Java Runtime Environment and the OpenJDK 21 Java Software Development Kit. For more information, see the OpenJDK documentation.

Jira:RHEL-51248

4.12. IDENTITY MANAGEMENT

python-jwcrypto rebased to version 1.5.6

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

Jira:RHELDOCS-18197[1]

The ldap_id_use_start_tls option is now enabled by default

To improve security, the default value for **ldap_id_use_start_tls** has changed from **false** to **true**. 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.

As unencrypted communication is not secure, the default **ldap_id_use_start_tls** option is now set to **true**.

Jira:RHELDOCS-19185[1]

certmonger rebased to version 0.79.20

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

- Enhanced handling of new certificates in the internal token and improved the removal process on renewal.

- Removed restrictions on tokens for **CKM_RSA_X_509** cryptographic mechanism.

- Fixed the documentation for the **getcert add-scep-ca**, **--ca-cert**, and **--ra-cert** options.

- Renamed the D-Bus service and configuration files to match canonical name.

- Added missing **.TP** tags in the **getcert-resubmit** man page.

- Migrated to the SPDX license format.

- Included owner and permissions information in the **getcert list** output.

- Removed the requirement for an NSS database in the **cm_certread_n_parse** function.

- Added translations using Webplate for Simplified Chinese, Georgian, and Russian.

Jira:RHEL-40922[1]

RHEL 10 provides **python-jwcrypto** in version 1.5.6

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

Jira:RHELDOCS-19191[1]

RHEL 10 provides **389-ds-base** package version 3.0.4

The **389-ds-base** package is now based on upstream version 3.0.4. Notable bug fixes and enhancements over previous versions are described in the upstream release notes:

- https://www.port389.org/docs/389ds/releases/release-3-0-1.html

- https://www.port389.org/docs/389ds/releases/release-3-0-4.html

Jira:RHEL-31780

389-ds-base now fully supports LMDB

Introduced in RHEL 9.5 as a Technology Preview, Lightning Memory-Mapped Database (LMDB) is now fully supported by the **389-ds-base** package in RHEL 10. Directory Server now creates instances with Lightning Memory-Mapped Database (LMDB) by default.

LMDB introduces the following configuration parameters that are stored under the new **cn=mdb,cn=config,cn=ldbm database,cn=plugins,cn=config** configuration entry:

- **nsslapd-mdb-max-size**. Sets the database maximum size in bytes.

Important

> Make sure that **nsslapd-mdb-max-size** is high enough to store all intended data. However, the parameter size must not be too high to impact the performance because the database file is memory-mapped.

- **nsslapd-mdb-max-readers**. Sets the maximum number of read operations that can be opened at the same time. Directory Server autotunes this setting.

- **nsslapd-mdb-max-dbs**. Sets the maximum number of named database instances that can be included within the memory-mapped database file.

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

The BDB instances are no longer supported. Therefore, migrate all instances to LMDB.

Jira:RHELDOCS-18966[1]

ansible-freeipa rebased to 1.13.2

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

- The **ansible-freeipa** package requires the **ansible-core** package version 2.15 minimum. Both **ansible-core** 2.15 and the latest version of **ansible-freeipa** are available in the Appstream repository. For this reason, no manual update of **ansible-core** is required.

- You can now create an inventory of Identity Management (IdM) servers for **ansible-freeipa** playbooks dynamically. The **freeipa** plugin gathers data about the IdM servers in the domain, and selects only those that have a specified IdM server role assigned. For example, if you want to search the logs of all IdM DNS servers in the domain to detect possible issues, the plugin ensures that all IdM replicas with the DNS server role are detected and automatically added to the managed nodes.

- You can now more efficiently run **ansible-freeipa** playbooks that use a single Ansible task to add, modify, and delete multiple Identity Management (IdM) users, user groups, hosts, and services. Previously, each entry in a list of users had its dedicated API call. With this enhancement, several API calls are combined into one API call within a task. The same applies to lists of user groups, hosts and services.
  As a result, the speed of adding, modifying, and deleting these IdM objects by using the **ipauser**, **ipagroup**, **ipahost** and **ipaservice** modules is increased. The biggest benefit can be seen when the client context is used.

- The **ansible-freeipa** rpm now installs the **freeipa.ansible_freeipa** collection only.
  To use the new collection, add the **freeipa.ansible_freeipa** prefix to the names of roles and modules. Use the fully-qualified names to follow Ansible recommendations. For example, to refer to the **ipahbacrule** module, use **freeipa.ansible_freeipa.ipahbacrule**.

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

Jira:RHEL-35566

4.13. SSSD

authselect is now required by PAM and cannot be uninstalled

With this enhancement, the **authselect-libs** package now owns **/etc/nsswitch.conf** and selected PAM configuration, including **system-auth**, **password-auth**, **smartcard-auth**, **fingerprint-auth**, and **postlogin** in **/etc/pam.d/**. Ownership of these files has been transferred to **authselect-libs** package, with **/etc/nsswitch.conf** previously owned by the **glibc** package and the PAM configuration files previously owned by the **pam** package. Since **authselect** is required by the **pam** package, it cannot be uninstalled.

For system upgrades from previous RHEL versions:

- If an **authselect** configuration already exists, **authselect apply-changes** automatically updates the configuration to the latest version. If there was no previous **authselect** configuration on your system, no changes are made.

- On systems managed by **authselect**, any non-authselect configurations are now forcefully overwritten without a prompt during the next **authselect** call. The **--force** option is no longer required.

If you require a special configuration, create a custom **authselect** profile. Note that you must manually update custom profiles to keep them up to date with your system.

You can opt-out from using **authselect**:

```
# authselect opt-out
```

Jira:RHELDOCS-19197

Local profile is the new default **authselect** profile

Due to the removal of the SSSD files provider, a new **authselect local** profile has been introduced to handle local user management without relying on SSSD. The **local** profile replaces the previous **minimal** profile and becomes the default **authselect** profile for new installations instead of the **sssd** profile.

During upgrades, the **authselect** utility automatically migrates existing configurations from **minimal** to **local** profile.

Additionally, the **sssd authselect** profile has been updated to remove the **with-files-domain** and **with-files-access-provider** options and it no longer handles local user accounts directly via these options. If you relied on these options, you must update your SSSD configuration to use **proxy provider** instead of **files provider**.

The **sssd** profile now supports the **--with-tlog** option, which enables session recording for users managed by SSSD.

Jira:RHELDOCS-19263[1]

Running SSSD with reduced privileges

To support general system hardening (running software with least privileges possible), the System Security Services Daemon (SSSD) service is now configured to run under **sssd** or **root** using the **systemd** service configuration files (service user). This service user now defaults to **sssd** and irrespective of what service user is configured, **root** or **sssd**, all root capabilities are dropped with the exception of a few privileged helper processes.

Note that you must ensure the correct ownership of configuration files. The **sssd.conf** file must be owned by the same user that is used to run the SSSD service. By default, in RHEL 10, this is the **sssd** user. If you create your **sssd.conf** file either manually or via an Ansible script, ensure the ownership is

correct. For example, if you create a **sssd.conf** file under the **root** user, you must change the ownership to **sssd:sssd** using the **chown** command.

Jira:RHELDOCS-18882[1]

Support for **KnownHostsCommand** has been added to SSSD

With this update, support for **KnownHostsCommand** has been added to SSSD. You can use the tool **sss_ssh_knownhosts** with the SSH **KnownHostsCommand** configuration option to retrieve the host's public keys from a remote server, such as FreeIPA, LDAP, and others. The **sss_ssh_knownhosts** tool replaces the less reliable **sss_ssh_knownhostsproxy** tool. **sss_ssh_knownhostsproxy** is no longer available and a message is displaying indicating the tool is obsolete.

Jira:RHELDOCS-19162[1]

4.14. DESKTOP

Firefox and Thunderbird are provided only as Flatpaks in RHEL 10

In RHEL 10.0 Beta, the Firefox Flatpak is not preinstalled. For RHEL 10.0, Firefox Flatpak will be automatically installed after the system is registered and is connected to the Internet.

To learn more about Flatpaks, see the Introducing the Red Hat Flatpak runtime for desktop containers Red Hat Blog article.

Install Firefox or Thunderbird on a RHEL 10-beta system by using the following steps:

1. Add the Flatpak registry to your system:

   ```
   # flatpak remote-add rhel-10-beta \
   https://flatpaks.redhat.io/rhel-10-beta.flatpakrepo
   ```

2. Log into the Red Hat Container Catalog:

   ```
   # podman login registry.redhat.io

   Username: <username>
   Password: <password>
   ```

   Provide the credentials to your Red Hat Customer Portal account or your registry service account tokens.

   By default, Podman saves the credentials only until you log out.

3. Optional: Save your credentials permanently. Use one of the following options:

   - Save the credentials for the current user:

     ```
     # cp $XDG_RUNTIME_DIR/containers/auth.json \
     $HOME/.config/flatpak/oci-auth.json
     ```

   - Save the credentials system-wide:

     ```
     # cp $XDG_RUNTIME_DIR/containers/auth.json \
     /etc/flatpak/oci-auth.json
     ```

When installing credentials system-wide, log into the Red Hat Container Catalog by using registry account tokens.

4. Install Firefox RHEL 10 Beta Flatpak

   ```
   # flatpak install rhel-10-beta org.mozilla.Firefox
   ```

5. Run Firefox from the GNOME overview or from the command line:

   ```
   # flatpak run org.mozilla.Firefox
   ```

Jira:RHEL-24332[1]

Window overview added to GNOME classic

In previous versions, the overview of open windows was not available while using the GNOME classic session. With this update, you can use the overview in both the standard GNOME and classic mode sessions. This makes the overview's features, including system search, available to classic mode users. Users can now also use classic mode extensions with the default GNOME session.

Jira:RHELDOCS-19060[1]

GNOME Online Accounts can restrict which features providers can use

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

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

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

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

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

Jira:RHEL-40831

4.15. THE WEB CONSOLE

New package: cockpit-files

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

- Browse files and directories on file systems you can access

- Sort files and directories by various criteria

- Filter displayed files by a sub-string

- Copy, move, delete, and rename files and directories

- Create directories

- Upload files

- Bookmark file paths

- Use keyboard shortcuts for the actions

Jira:RHELDOCS-16362[1]

4.16. RED HAT ENTERPRISE LINUX SYSTEM ROLES

Support for new ha_cluster system role features

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

- Configuring utilization attributes for node and primitive resources.

- Configuring node addresses and SBD options by using the **ha_cluster_node_options** variable. If both **ha_cluster_node_options** and **ha_cluster** variables are defined, their values are merged, with values from **ha_cluster_node_options** having precedence.

- Configuring access control lists (ACLs).

- Configuring Pacemaker alerts to take an external action when a cluster event such as node failure or resource starting or stopping occurs.

- Easy installation of agents for cloud environments by setting the **ha_cluster_install_cloud_agents** variable to **true**.

Jira:RHEL-34893[1], Jira:RHEL-34898, Jira:RHEL-34894, Jira:RHEL-34885

New sudo RHEL system role

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

Jira:RHEL-37551

The storage RHEL system role can now manage Stratis pools

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

- Create a new encrypted and unencrypted Stratis pool

- Add new volumes to the existing Stratis pool

- Add new disks to the Stratis pool

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

Jira:RHEL-40798[1]

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

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

- **podman_registry_certificates** (list of dictionary elements): Enables you to manage TLS certificates and keys used to connect to the specified container image registry.

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

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

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

Jira:RHEL-34884[1]

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

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

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

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

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

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

Jira:RHEL-34890[1]

New variable in the **podman** RHEL system role: **podman_credential_files**

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

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

podman_credential_files (list of dictionary elements)

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

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

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

Jira:RHEL-34891[1]

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

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

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

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

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

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

Jira:RHEL-34892[1]

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

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

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

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

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

```
- name: Non-exclusive sshd configuration
  hosts: managed-node-01.example.com
  tasks:
    - name: Configure ssh to obscure keystroke timing and set 5m session timeout
      ansible.builtin.include_role:
```

```
    name: rhel-system-roles.ssh
    vars:
      ssh_ObscureKeystrokeTiming: _"interval:80"_
      ssh_ChannelTimeout: _"session=5m"_
```

Jira:RHEL-40181

The storage RHEL system role can now resize LVM physical volumes

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

Jira:RHEL-40797[1]

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

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

- Initial ramdisk

- NetworkManager flush module

- Dracut flush module

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

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

Jira:RHEL-45718[1]

New variable in the postfix RHEL system role: postfix_files

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

postfix_files

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

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

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

Jira:RHEL-46855[1]

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

With thin provisioning, you can use the **snapshot** RHEL system role to manage snapshots of LVM thin pools. These thin snapshots are space-efficient and only grow as data is written or modified after the

snapshot is taken. The role automatically detects if the specified volume is scheduled for a thin pool. The added feature could be useful in environments where you need to take frequent snapshots without consuming a lot of physical storage.

Jira:RHEL-48230[1]

New option in the logging RHEL system role: reopen_on_truncate

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

reopen_on_truncate (boolean, defaults to false)

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

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

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

Jira:RHEL-48609[1]

New variable in the logging RHEL system role: logging_custom_config_files

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

logging_custom_config_files (list)

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

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

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

Jira:RHEL-50288[1]

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

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

- **mode** (raw, defaults to null): Configures the **FileCreateMode** parameter associated with the **omfile** module in the **rsyslog** service.

- **owner** (string, defaults to null): Configures the **fileOwner** or **fileOwnerNum** parameter associated with the **omfile** module in **rsyslog**. If the value is an integer, it sets **fileOwnerNum**. Otherwise, it sets **fileOwner**.

- **group** (string, defaults to null): Configures the **fileGroup** or **fileGroupNum** parameter associated with the **omfile** module in **rsyslog**. If the value is an integer, it sets **fileGroupNum**. Otherwise, it sets **fileGroup**.

- **dir_mode** (defaults to null): Configures the **DirCreateMode** parameter associated with the **omfile** module in **rsyslog**.

- **dir_owner** (defaults to null): Configures the **dirOwner** or **dirOwnerNum** parameter associated with the **omfile** module in **rsyslog**. If the value is an integer, it sets **dirOwnerNum**. Otherwise, it sets **dirOwner**.

- **dir_group** (defaults to null): Configures the **dirGroup** or **dirGroupNum** parameter associated with the **omfile** module in **rsyslog**. If the value is an integer, it sets **dirGroupNum**. Otherwise, it sets **dirGroup**.

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

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

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

Jira:RHEL-50289[1]

Using the **storage** RHEL system role creates fingerprints on managed nodes

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

Jira:RHEL-50291[1]

New **src** parameter is added to the **network** RHEL system role

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

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

Jira:RHEL-53901[1]

Support for configuring GFS2 file systems on RHEL 9 clusters by using RHEL system roles

Red Hat Enterprise Linux 10 supports the configuration and management of the Red Hat Global File System 2 (GFS2) by using the **gfs2** RHEL system role on a RHEL 10 control node to manage RHEL 9 systems. The Red Hat Enterprise Linux (RHEL) Resilient Storage Add-On, which includes the GFS2 file system, is itself not supported on RHEL 10 systems. The role creates GFS2 file systems in a Pacemaker cluster managed with the **pcs** command-line interface.

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

The gfs2 role performs the following tasks:

- Installing the packages necessary for configuring a GFS2 file system in a Red Hat high availability cluster

- Setting up the **dlm** and **lvmlockd** cluster resources

- Creating the LVM volume groups and logical volumes required by the GFS2 file system

- Creating the GFS2 file system and cluster resources with the necessary resource constraints

Jira:RHEL-34828[1]

4.17. VIRTUALIZATION

nbdkit rebased to version 1.38

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

- Block size advertising has been enhanced and a new read-only filter has been added.

- The Python and OCaml bindings support more features of the server API.

- Internal struct integrity checks have been added to make the server more robust.

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

Jira:RHEL-32748

4.18. RHEL IN CLOUD ENVIRONMENTS

cloud-init now uses NetworkManager as the default network renderer

With this update, the **cloud-init** utility uses **NetworkManager** (NM) as the back end for network configuration when initializing a cloud instance. As a result, using NM keyfiles in **cloud-init** setup no longer requires reconfiguring **/etc/cloud/cloud.cfg**.

Jira:RHEL-29720[1]

4.19. 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]

4.20. CONTAINERS

Image mode for RHEL now supports FIPS mode

With this enhancement, you can enable the FIPS mode when building a bootc image to configure the system to use only FIPS-approved modules. You can use **bootc-image-builder**, which requires enabling the FIPS crypto policy in the Containerfile configuration, or use the RHEL Anaconda installation, that additionally to enabling FIPS mode in the Containerfile, also requires adding the **fips=1** kernel argument when booting the system installation. See Installing the system with FIPS mode enabled for more details.

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

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

Jira:RHELDOCS-18585[1]

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

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

Jira:RHELDOCS-18398[1]

Podman and Buildah support adding OCI artifacts to image indexes

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

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

- the **--artifact** option to create artifact manifests

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

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

- the **--index** option to set annotations on the index itself instead of a one of the entries in the image index

- the **--subject** option for setting the subject field of an image index.

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

Option is available to disable Podman healthcheck event

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

Runtime resource changes in Podman are persistent

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

Building multi-architecture images is fully supported

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

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

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

- Build an image on all nodes in a farm.

- Bundle an image on all nodes in a farm up into a manifest list.

- Execute the **podman build** command on all the farm nodes.

- Push the images to the registry specified by using the **--tag** option.

- Locally create a manifest list.

- Push the manifest list to the registry.

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

Quadlets for pods in Podman are available

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

The Podman v2.0 RESTful API has been updated

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

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

- The **os** and **arch** fields for image listing.

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

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

The Container Tools packages have been updated

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

- The **podman manifest add** command now supports a new **--artifact** option to add OCI artifacts to a manifest list.

- The **podman create**, **podman run**, and **podman push** commands now support the **--retry** and **--retry-delay** options to configure retries for pushing and pulling images.

- The **podman run** and **podman exec** commands now support the **--preserve-fd** option to pass a list of file descriptors into the container. It is an alternative to **--preserve-fds**, which passes a specific number of file descriptors.

- Quadlet now supports templated units.

- The **podman kube play** command can now create image-based volumes by using the **volume.podman.io/image** annotation.

- Containers created with the **podman kube play** command can now include volumes from other containers by using a new annotation, **io.podman.annotations.volumes-from**.

- Pods created with the **podman kube play** command can now set user namespace options by using the **io.podman.annotations.userns annotation** in the pod definition.

- The **--gpus** option to **podman create** and **podman run** is now compatible with Nvidia GPUs.

- The **--mount** option to **podman create** and **podman run** supports a new mount option, **no-dereference**, to mount a symlink instead of its dereferenced target into a container.

- Podman now supports the new **--config** global option to point to a Docker configuration where registry login credentials can be sourced.

- The **podman ps --format** command now supports the new **.Label** format specifier.

- The **uidmapping** and **gidmapping** options to the **podman run --userns=auto** option can now map to host IDs by prefixing host IDs with the @ symbol.

- Quadlet now supports systemd-style drop-in directories.

- Quadlet now supports creating pods by using the new **.pod** unit files.

- Quadlet now supports two new keys, **Entrypoint** and **StopTimeout**, in **.container** files.

- Quadlet now supports specifying the **Ulimit** key multiple times in **.container** files to set more than one **ulimit** on a container.

- Quadlet now supports setting the **Notify** key to **healthy** in **.container** files, to only notify that a container has started when its health check begins passing.

- The output of the **podman inspect** command for containers has changed. The **Entrypoint** field changes from a string to an array of strings and **StopSignal** from an integer to a string.

- The **podman inspect** command for containers now returns nil for health checks when inspecting containers without health checks.

- It is no longer possible to create new BoltDB databases. Attempting to do so results in an error. All new Podman installations now use the SQLite database backend. Existing BoltDB databases remain usable.

- Support for CNI networking is gated by a build tag and is not enabled by default.

- Podman now prints warnings when used on **cgroups v1** systems. Support for **cgroups v1** is deprecated and will be removed in a future release. You can set the **PODMAN_IGNORE_CGROUPSV1_WARNING** environment variable to suppress warnings.

- Network statistics sent over the Docker-compatible API are now per-interface, and not aggregated, which improves Docker compatibility.

- The default tool for rootless networking has been changed from **slirp4netns** to **pasta** for improved performance. As a result, networks named **pasta** are no longer supported.

- Using multiple filters with the List Images REST API now combines the filters with AND instead of OR, improving Docker compatibility.

- The parsing for a number of Podman CLI options which accept arrays has been changed to no longer accept string-delimited lists, and instead to require the option to be passed multiple times. These options are:

  - The **--annotation** option to **podman manifest annotate** and **podman manifest add**

  - The **--configmap**, **--log-opt**, and **--annotation** options to **podman kube play**

- The **--pubkeysfile** option to **podman image trust set**

  - The **--encryption-key** and **--decryption-key** options to **podman create**, **podman run**, **podman push** and **podman pull**

  - The **--env-file** option to **podman exec**, the **--bkio-weight-device**, **--device-read-bps**, **--device-write-bps**, **--device-read-iops**, **--device-write-iops**, **--device**, **--label-file**, **--chrootdirs**, **--log-opt**, **--env-file** options to **podman create** and **podman run**

  - The **--hooks-dir** and **--module** global options

- The **podman system reset** command no longer waits for running containers to stop, and instead immediately sends the **SIGKILL** signal.

- The **podman network inspect** command now includes running containers that use the network in its output.

- The **podman compose** command is now supported on other architectures in addition to AMD and Intel 64-bit architectures (x86-64-v2) and the 64-bit ARM architecture (ARMv8.0-A)..

- The **--no-trunc** option to the **podman kube play** and **podman kube generate** commands has been deprecated. Podman now complies to the Kubernetes specification for annotation size, which removes the need for this option.

- Connections from the **podman system connection** command and farms from the **podman farm** command are now written to a new configuration file called **podman-connections.conf** file. As a result, Podman no longer writes to the **containers.conf** file. Podman still respects existing connections from **containers.conf**.

- Most **podman farm** subcommands no longer need to connect to the machines in the farm to run.

- The **podman create** and **podman run** commands no longer require specifying an entrypoint on the command line when the container image does not define one. In this case, an empty command is passed to the OCI runtime, and the resulting behavior is runtime-specific.

- A new API endpoint, **/libpod/images/$name/resolve**, has been added to resolve a potential short name to a list of fully-qualified image references Podman, which you can use to pull the image.

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

Jira:RHEL-32715

The containers.conf file is now read-only

The system connections and farm information stored in the **containers.conf** file is now read-only. The system connections and farm information will now be stored in the **podman.connections.json** file, managed only by Podman. Podman continues to support the old configuration options such as **[engine.service_destinations]** and the **[farms]** section. You can still add connections or farms manually if needed however, it is not possible to delete a connection from the **containers.conf** file with the **podman system connection rm** command.

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

Jira:RHEL-40639

Default settings changes for Podman v5.0

In RHEL 10.0 Beta, the following default settings changes for Podman v5.0:

- cgroups v2 is used by default instead of cgroups v1

- **pasta** is the default network used by rootless containers instead of **slirp4netns**

Jira:RHEL-40643

A new rhel10-beta/rteval container image

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

Jira:RHELDOCS-18522[1]

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

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

Jira:RHEL-52240

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

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

Jira:RHELDOCS-18769[1]

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

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

Jira:RHELDOCS-18472[1]

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

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

Jira:RHELDOCS-18770[1]

CHAPTER 5. IMPORTANT CHANGES TO EXTERNAL KERNEL PARAMETERS

This chapter provides system administrators with a summary of significant changes in the kernel distributed with Red Hat Enterprise Linux 10.0 Beta. 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

accept_memory=

[MM]

Values:

lazy (default)

> By default, unaccepted memory is accepted lazily to avoid prolonged boot times. The lazy option adds some runtime overhead until all memory is eventually accepted. In most cases, the overhead is negligible.

eager

> For some workloads or for debugging purposes, you can use **accept_memory=eager** to accept all memory at once during boot.

arm64.nomops

[ARM64]

Unconditionally disable Memory Copy and Memory Set instructions support.

cgroup_favordynmods=

[KNL]

Enable or disable **favordynmods**.

Values:

- **true**

- **false**

Defaults to the value of **CONFIG_CGROUP_FAVOR_DYNMODS**.

early_page_ext

[KNL]

Enforces **page_ext** initialization to earlier stages to cover more early boot allocations.

Note that as side effect, some optimizations might be disabled to achieve that: for example, parallelized memory initialization is disabled. Therefore, the boot process might take longer, especially on systems with much memory.

Available with **CONFIG_PAGE_EXTENSION=y**.

fw_devlink.sync_state=

[KNL]

When all devices that could probe have finished probing, this parameter controls what to do with devices that have not yet received their **sync_state()** calls.

Values:

strict (default)

Continue waiting on consumers to probe successfully.

timeout

Give up waiting on consumers and call **sync_state()** on any devices that have not yet received their **sync_state()** calls after **deferred_probe_timeout** has expired or by **late_initcall()** if **CONFIG_MODULES** is **false**.

ia32_emulation=

[X86-64]

Values:

true

Allows loading 32-bit programs and executing 32-bit syscalls, essentially overriding **IA32_EMULATION_DEFAULT_DISABLED** at boot time.

false

Unconditionally disables IA32 emulation.

kunit.enable=

[KUNIT]

Enable executing KUnit tests. Requires **CONFIG_KUNIT** to be set to be fully enabled.

You can override the default value using **KUNIT_DEFAULT_ENABLED**.

The default is 1 (enabled).

mtrr=debug

[X86]

Enable printing debug information related to MTRR registers at boot time.

rcupdate.rcu_cpu_stall_cputime=

[KNL]

Provide statistics on the CPU time and count of interrupts and tasks during the sampling period. For multiple continuous RCU stalls, all sampling periods begin at half of the first RCU stall timeout.

rcupdate.rcu_exp_stall_task_details=

[KNL]

Print stack dumps of any tasks blocking the current expedited RCU grace period during an expedited RCU CPU stall warning.

spec_rstack_overflow=

[X86]

Control RAS overflow mitigation on AMD Zen CPUs.

Values:

off

Disable mitigation

microcode

Enable only microcode mitigation.

safe-ret (default)

Enable software-only safe RET mitigation.

ibpb

Enable mitigation by issuing IBPB on kernel entry.

ibpb-vmexit

Issue IBPB only on VMEXIT. This mitigation is specific to cloud environments.

workqueue.unbound_cpus=

[KNL,SMP]

Specify to constrain one or some CPUs to use in unbound workqueues.

Value: A list of CPUs.

By default, all online CPUs are available for unbound workqueues.

Updated kernel parameters

amd_iommu=

[HW, X86-64]

Pass parameters to the AMD IOMMU driver in the system.

Values:

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.

New: **pgtbl_v1** (default)

Use version 1 page table for DMA-API.

New: **pgtbl_v2**

Use version 2 page table for DMA-API.

New: irtcachedis

Disable Interrupt Remapping Table (IRT) caching.

nosmt

[KNL, **PPC**, S390]

Disable symmetric multithreading (SMT). Equivalent to **smt=1**.

[KNL, X86, **PPC**]

Disable symmetric multithreading (SMT).

nosmt=force

Force disable SMT. Cannot be undone using the **sysfs** control file.

page_reporting.page_reporting_order=

[KNL]

Minimal page reporting order.

Value: integer.

Adjust the minimal page reporting order.

New: The page reporting is disabled when it exceeds   **MAX_ORDER**.

tsc=

Disable clocksource stability checks for TSC.

Values:

[x86] reliable

Mark tsc clocksource as reliable. This disables clocksource verification at runtime, and the stability checks done at bootup. Used to enable high-resolution timer mode on older hardware, and in virtualized environment.

[x86] noirqtime

Do not use TSC to do **irq** accounting. Used to run time disable   **IRQ_TIME_ACCOUNTING** on any platforms where RDTSC is slow and this accounting might add overhead.

[x86] unstable

Mark the TSC clocksource as unstable. This marks the TSC unconditionally unstable at bootup and avoids any further wobbles once the TSC watchdog notices.

[x86] nowatchdog

Disable clocksource watchdog. Used in situations with strict latency requirements, where interruptions from clocksource watchdog are not acceptable.

[x86] recalibrate

Force recalibration against a HW timer (HPET or PM timer) on systems whose TSC frequency was obtained from HW or FW using either an MSR or CPUID(0x15). Warn if the difference is more than 500 ppm.

New: [x86]watchdog

Use TSC as the watchdog clocksource with which to check other HW timers (HPET or PM timer), but only on systems where TSC has been deemed trustworthy.
An earlier **tsc=nowatchdog** suppresses this. A later **tsc=nowatchdog** overrides this. A console message flags any such suppression or overriding.

usbcore.authorized_default=

[USB]

Default USB device authorization.

Values:

New: -1 (default)

Authorized (same as 1).

0

Not authorized.

1

Authorized.

2

Authorized if the device connects to an internal port.

Removed kernel parameters

- **cpu0_hotplug**

- **sysfs.deprecated**

New sysctl parameters

io_uring_group

Values:

1

A process must either be privileged (**CAP_SYS_ADMIN**) or be in the **io_uring_group** group to create an **io_uring** instance.

-1 (default)

Only processes with the **CAP_SYS_ADMIN** capability can create **io_uring** instances.

numa_balancing_promote_rate_limit_MBps

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

A rule of thumb is to set this to less than 1/10 of the PMEM node write bandwidth.

Updated sysctl parameters

io_uring_disabled

Prevents all processes from creating new **io_uring** instances. Enabling this shrinks the attack surface of the kernel.

Values:

New: 0

> All processes can create **io_uring** instances as normal.

New: 1

> **io_uring** creation is disabled for unprivileged processes not in the io_uring_group group.
> **io_uring_setup()** fails with **-EPERM**. Existing **io_uring** instances can still be used.
> See the documentation for **io_uring_group** for more information.

New: 2 (default)

> **io_uring** creation is disabled for all processes. **io_uring_setup()** always fails with **-EPERM**. Existing **io_uring** instances can still be used.

CHAPTER 6. DEVICE DRIVERS

6.1. NEW DRIVERS

Table 6.1. Cryptographic drivers

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

Table 6.2. Network drivers

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

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

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

Table 6.3. Platform drivers

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

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

Table 6.4. Graphics drivers and miscellaneous drivers

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

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

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

6.2. UPDATED DRIVERS

Table 6.5. Storage driver updates

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

CHAPTER 7. AVAILABLE BPF FEATURES

This chapter provides the complete list of Berkeley Packet Filter (BPF) features available in the kernel of this minor version of Red Hat Enterprise Linux 10-beta. The tables include the lists of:

- System configuration and other options

- Available program types and supported helpers

- Available map types

This chapter contains automatically generated output of the **bpftool feature** command.

Table 7.1. System configuration and other options

Option	Value
unprivileged_bpf_disabled	2 (bpf() syscall restricted to privileged users, admin can change)
JIT enable	1 (enabled)
JIT harden	1 (enabled for unprivileged users)
JIT kallsyms	1 (enabled for root)
Memory limit for JIT for unprivileged users	69267617742848
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	n
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	100
bpf() syscall	available
Large insn size limit	available
Bounded loop support	available
ISA extension v2	available
ISA extension v3	available

Table 7.2. Available program types and supported helpers

Program type	Available helpers
socket_filter	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_perf_event_output, bpf_skb_load_bytes, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_skb_load_bytes_relative, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
kprobe	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_copy_from_user, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_task_storage_get, bpf_task_storage_delete, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_get_func_ip, bpf_get_attach_cookie, bpf_task_pt_regs, bpf_get_branch_snapshot, bpf_find_vma, bpf_loop, bpf_strncmp, bpf_copy_from_user_task, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
sched_cls	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_l3_csum_replace, bpf_l4_csum_replace, bpf_tail_call, bpf_clone_redirect, bpf_get_cgroup_classid, bpf_skb_vlan_push, bpf_skb_vlan_pop, bpf_skb_get_tunnel_key, bpf_skb_set_tunnel_key, bpf_redirect, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_get_tunnel_opt, bpf_skb_set_tunnel_opt, bpf_skb_change_proto, bpf_skb_change_type, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_change_tail, bpf_skb_pull_data, bpf_csum_update, bpf_set_hash_invalid, bpf_get_numa_node_id, bpf_skb_change_head, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_set_hash, bpf_skb_adjust_room, bpf_skb_get_xfrm_state, bpf_skb_load_bytes_relative, bpf_fib_lookup, bpf_skb_cgroup_id, bpf_get_current_cgroup_id, bpf_skb_ancestor_cgroup_id, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sk_fullsock, bpf_tcp_sock, bpf_skb_ecn_set_ce, bpf_get_listener_sock, bpf_skc_lookup_tcp, bpf_tcp_check_syncookie, bpf_strtol, bpf_strtoul, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_tcp_gen_syncookie, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_sk_assign, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_csum_level, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_skb_cgroup_classid, bpf_redirect_neigh, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_redirect_peer, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_check_mtu, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_skb_set_tstamp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_tcp_raw_gen_syncookie_ipv4, bpf_tcp_raw_gen_syncookie_ipv6, bpf_tcp_raw_check_syncookie_ipv4, bpf_tcp_raw_check_syncookie_ipv6, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
sched_act	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_l3_csum_replace, bpf_l4_csum_replace, bpf_tail_call, bpf_clone_redirect, bpf_get_cgroup_classid, bpf_skb_vlan_push, bpf_skb_vlan_pop, bpf_skb_get_tunnel_key, bpf_skb_set_tunnel_key, bpf_redirect, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_get_tunnel_opt, bpf_skb_set_tunnel_opt, bpf_skb_change_proto, bpf_skb_change_type, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_change_tail, bpf_skb_pull_data, bpf_csum_update, bpf_set_hash_invalid, bpf_get_numa_node_id, bpf_skb_change_head, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_set_hash, bpf_skb_adjust_room, bpf_skb_get_xfrm_state, bpf_skb_load_bytes_relative, bpf_fib_lookup, bpf_skb_cgroup_id, bpf_get_current_cgroup_id, bpf_skb_ancestor_cgroup_id, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sk_fullsock, bpf_tcp_sock, bpf_skb_ecn_set_ce, bpf_get_listener_sock, bpf_skc_lookup_tcp, bpf_tcp_check_syncookie, bpf_strtol, bpf_strtoul, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_tcp_gen_syncookie, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_sk_assign, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_csum_level, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_skb_cgroup_classid, bpf_redirect_neigh, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_redirect_peer, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_check_mtu, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_skb_set_tstamp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_tcp_raw_gen_syncookie_ipv4, bpf_tcp_raw_gen_syncookie_ipv6, bpf_tcp_raw_check_syncookie_ipv4, bpf_tcp_raw_check_syncookie_ipv6, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
tracepoint	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_copy_from_user, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_task_storage_get, bpf_task_storage_delete, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_get_func_ip, bpf_get_attach_cookie, bpf_task_pt_regs, bpf_get_branch_snapshot, bpf_find_vma, bpf_loop, bpf_strncmp, bpf_copy_from_user_task, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
xdp	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_redirect, bpf_perf_event_output, bpf_csum_diff, bpf_get_current_task, bpf_get_numa_node_id, bpf_xdp_adjust_head, bpf_redirect_map, bpf_xdp_adjust_meta, bpf_xdp_adjust_tail, bpf_fib_lookup, bpf_get_current_cgroup_id, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_skc_lookup_tcp, bpf_tcp_check_syncookie, bpf_strtol, bpf_strtoul, bpf_tcp_gen_syncookie, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_check_mtu, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_xdp_get_buff_len, bpf_xdp_load_bytes, bpf_xdp_store_bytes, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_tcp_raw_gen_syncookie_ipv4, bpf_tcp_raw_gen_syncookie_ipv6, bpf_tcp_raw_check_syncookie_ipv4, bpf_tcp_raw_check_syncookie_ipv6, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
perf_event	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_perf_prog_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_read_branch_records, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_copy_from_user, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_task_storage_get, bpf_task_storage_delete, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_get_func_ip, bpf_get_attach_cookie, bpf_task_pt_regs, bpf_get_branch_snapshot, bpf_find_vma, bpf_loop, bpf_strncmp, bpf_copy_from_user_task, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
cgroup_skb	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_perf_event_output, bpf_skb_load_bytes, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_skb_load_bytes_relative, bpf_skb_cgroup_id, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_skb_ancestor_cgroup_id, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sk_fullsock, bpf_tcp_sock, bpf_skb_ecn_set_ce, bpf_get_listener_sock, bpf_skc_lookup_tcp, bpf_strtol, bpf_strtoul, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_sk_cgroup_id, bpf_sk_ancestor_cgroup_id, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
cgroup_sock	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_get_cgroup_classid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_sk_storage_get, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_netns_cookie, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_loop, bpf_strncmp, bpf_get_retval, bpf_set_retval, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
lwt_in	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_cgroup_classid, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_pull_data, bpf_get_numa_node_id, bpf_lwt_push_encap, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
lwt_out	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_cgroup_classid, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_pull_data, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
lwt_xmit	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_l3_csum_replace, bpf_l4_csum_replace, bpf_tail_call, bpf_clone_redirect, bpf_get_cgroup_classid, bpf_skb_get_tunnel_key, bpf_skb_set_tunnel_key, bpf_redirect, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_get_tunnel_opt, bpf_skb_set_tunnel_opt, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_change_tail, bpf_skb_pull_data, bpf_csum_update, bpf_set_hash_invalid, bpf_get_numa_node_id, bpf_skb_change_head, bpf_lwt_push_encap, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_csum_level, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
sock_ops	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_setsockopt, bpf_sock_map_update, bpf_getsockopt, bpf_sock_ops_cb_flags_set, bpf_sock_hash_update, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_tcp_sock, bpf_strtol, bpf_strtoul, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_netns_cookie, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_load_hdr_opt, bpf_store_hdr_opt, bpf_reserve_hdr_opt, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
sk_skb	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_tail_call, bpf_perf_event_output, bpf_skb_load_bytes, bpf_get_current_task, bpf_skb_change_tail, bpf_skb_pull_data, bpf_get_numa_node_id, bpf_skb_change_head, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_skb_adjust_room, bpf_sk_redirect_map, bpf_sk_redirect_hash, bpf_get_current_cgroup_id, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_skc_lookup_tcp, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
cgroup_device	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_get_cgroup_classid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
sk_msg	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_cgroup_classid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_msg_redirect_map, bpf_msg_apply_bytes, bpf_msg_cork_bytes, bpf_msg_pull_data, bpf_msg_redirect_hash, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_msg_push_data, bpf_msg_pop_data, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_netns_cookie, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
raw_tracepoint	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_copy_from_user, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_task_storage_get, bpf_task_storage_delete, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_get_func_ip, bpf_task_pt_regs, bpf_get_branch_snapshot, bpf_find_vma, bpf_loop, bpf_strncmp, bpf_copy_from_user_task, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
cgroup_sock_addr	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_get_cgroup_classid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_setsockopt, bpf_getsockopt, bpf_bind, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_skc_lookup_tcp, bpf_strtol, bpf_strtoul, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_netns_cookie, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_get_retval, bpf_set_retval, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
lwt_seg6local	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_cgroup_classid, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_pull_data, bpf_get_numa_node_id, bpf_lwt_seg6_store_bytes, bpf_lwt_seg6_adjust_srh, bpf_lwt_seg6_action, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
lirc_mode2	not supported
sk_reuseport	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_skb_load_bytes, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_skb_load_bytes_relative, bpf_get_current_cgroup_id, bpf_sk_select_reuseport, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
flow_dissector	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_skb_load_bytes, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
cgroup_sysctl	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_get_cgroup_classid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sysctl_get_name, bpf_sysctl_get_current_value, bpf_sysctl_get_new_value, bpf_sysctl_set_new_value, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
raw_tracepoint_writable	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_copy_from_user, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_task_storage_get, bpf_task_storage_delete, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_get_func_ip, bpf_task_pt_regs, bpf_get_branch_snapshot, bpf_find_vma, bpf_loop, bpf_strncmp, bpf_copy_from_user_task, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
cgroup_sockopt	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_get_cgroup_classid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_tcp_sock, bpf_strtol, bpf_strtoul, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_netns_cookie, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_loop, bpf_strncmp, bpf_get_retval, bpf_set_retval, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
tracing	
struct_ops	
ext	
lsm	

Program type	Available helpers
sk_lookup	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_sk_assign, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
syscall	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_get_socket_cookie, bpf_perf_event_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_send_signal, bpf_skb_output, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_xdp_output, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_get_task_stack, bpf_d_path, bpf_copy_from_user, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_task_storage_get, bpf_task_storage_delete, bpf_get_current_task_btf, bpf_sock_from_file, bpf_for_each_map_elem, bpf_snprintf, bpf_sys_bpf, bpf_btf_find_by_name_kind, bpf_sys_close, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_get_func_ip, bpf_task_pt_regs, bpf_get_branch_snapshot, bpf_skc_to_unix_sock, bpf_kallsyms_lookup_name, bpf_find_vma, bpf_loop, bpf_strncmp, bpf_xdp_get_buff_len, bpf_copy_from_user_task, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
netfilter	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Table 7.3. Available map types

Map type	Available
hash	yes
array	yes
prog_array	yes
perf_event_array	yes
percpu_hash	yes
percpu_array	yes
stack_trace	yes
cgroup_array	yes
lru_hash	yes
lru_percpu_hash	yes
lpm_trie	yes
array_of_maps	yes
hash_of_maps	yes

Map type	Available
devmap	yes
sockmap	yes
cpumap	yes
xskmap	yes
sockhash	yes
cgroup_storage	yes
reuseport_sockarray	yes
percpu_cgroup_storage	yes
queue	yes
stack	yes
sk_storage	yes
devmap_hash	yes
struct_ops	yes
ringbuf	yes
inode_storage	yes
task_storage	yes
bloom_filter	yes
user_ringbuf	yes
cgrp_storage	yes

CHAPTER 8. FIXED ISSUES

This version provides the following bug fixes and resolves issues and other problems that have a significant impact.

8.1. SECURITY

IPsec **ondemand** connections no longer fail to establish

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

Jira:RHEL-51880[1]

NSS now enforce EMS in FIPS mode

The Network Security Services (NSS) libraries now contain the **TLS-REQUIRE-EMS** keyword to require the Extended Master Secret (EMS) extension (RFC 7627) for all TLS 1.2 connections as mandated by the FIPS 140-3 standard. NSS use the new keyword when the system-wide cryptographic policies are set to **FIPS**.

If your scenario requires interoperating with legacy systems without support for EMS or TLS 1.3, you can apply the **NO-ENFORCE-EMS** system-wide cryptographic subpolicy. However, this change violates the FIPS-140-3 requirements.

Jira:RHEL-36299

Binary tests for **libcap** are waived

The **annocheck** tool discovered binary packages in the **libcap** library function that were built without the required flags for RHEL 10 architectures. We examined the flags for potential problems and did not find any. After careful investigation, we have waived the results for **libcap**. As a result, all tests for **libcap** passed.

Jira:RHEL-33498[1]

8.2. SHELLS AND COMMAND-LINE TOOLS

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

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

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

> ERROR: Invalid scheme '' in BACKUP_URL

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

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

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

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

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

Jira:RHEL-46613[1]

8.3. HIGH AVAILABILITY AND CLUSTERS

pcs validation of SBD options

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

Jira:RHEL-38484[1]

Ability to remove Booth configuration from a Booth arbitrator node

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

Jira:RHEL-38486[1]

pcsd processes now consistently stop correctly and promptly

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

Jira:RHEL-38478[1]

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

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

Jira:RHEL-38479[1]

The syntax for specifying a scorevalue is now consistent across all   pcs constraint commands

Previously, some commands for creating constraints required you to specify a score value as

score=_value_, whereas others expected just _value_ without **score=**. With this update, all constraint commands accept a score value in the form **score=**_value_, with the exception of **pcs constraint location prefers** and **pcs constraint location avoids**, which expect _node=score_ where _score_ is the score value.

Jira:RHEL-34792[1]

8.4. IDENTITY MANAGEMENT

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

Previously, the **ipa idrange-add** command did not warn the administrator that they must restart the Directory Server (DS) service on all IdM servers after creating a new range. As a consequence, the administrator sometimes created a new user or group with a UID or GID belonging to the new range without restarting the DS service. The addition resulted in the new user or group not having an SID assigned. With this update, a warning that DS needs to be restarted on all IdM servers is added to the command output.

Jira:RHELDOCS-18201[1]

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

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

Jira:RHEL-4879

certmonger now correctly renews KDC certificates on hidden replicas

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

Jira:RHEL-46607[1]

8.5. SSSD

sssd-polkit-rules package content moved to **sssd-common**

Previously, if you needed to enable smart card support when the system security services daemon (SSSD) did not run as **root**, you had to install the **sssd-polkit-rules** package. The package provided **polkit** integration with SSSD. To resolve this issue, the **sssd-common** package now includes the content of the **sssd-polkit-rules** package and installation of a separate package is no longer required.

Jira:RHEL-50243

8.6. RED HAT ENTERPRISE LINUX SYSTEM ROLES

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

Running the **sshd** RHEL system role to configure the second **sshd** service on your managed nodes

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

Jira:RHEL-34879[1]

No property conflicts between the NetworkManager service and the NetworkManager plugin

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

Jira:RHEL-34887[1]

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

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

Jira:RHEL-34886[1]

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

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

Jira:RHEL-34881[1]

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

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

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

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

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

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

Jira:RHEL-34888[1]

The linger feature can be canceled for the correct users

When processing the instruction list of configuration items from kube files or Quadlet files, the **podman** RHEL system role was incorrectly using the user ID associated with the entire list. It did not use the user ID associated with the list item to compile the linger file name. Consequently, the linger file was not created and therefore the **podman** RHEL system role could not cancel the linger feature for the actual user if necessary. With this update, **podman** uses the correct username to construct the linger file name. As a result, the linger feature can be canceled for the correct users.

Jira:RHEL-34889[1]

The **storage** RHEL system role is idempotent again

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

Jira:RHEL-34895[1]

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

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

Jira:RHEL-34907[1]

You cannot set the **name** parameter for the **imuxsock** input type

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

Jira:RHEL-38456

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

Previously, the **bootloader** RHEL system role incorrectly placed the password information in the **/boot/efi/EFI/redhat/user.cfg** file on managed nodes that ran RHEL 10 Beta and RHEL 9 with UEFI Secure Boot feature. The correct location was the **/boot/grub2/user.cfg** file. Consequently, when you rebooted the managed node to modify any boot loader entry, GRUB2 did not prompt you for a

password. This update fixes the problem by setting the path for **user.cfg** to **/boot/grub2/** in the source code. When you reboot the OS on a UEFI Secure Boot managed node to modify any boot loader entry, GRUB2 prompts you to input your password.

Jira:RHEL-40759[1]

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

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

Jira:RHEL-40760

The **podman** RHEL system role creates new secrets if necessary

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

Jira:RHEL-40795[1]

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

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

Jira:RHEL-50104[1]

The **podman** RHEL system role now correctly searches for subgid values

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

Jira:RHEL-57100[1]

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

Previously, the **dnf** module used through the **cockpit** RHEL system role did not install all **cockpit**-related packages. As a consequence, some requested packages were not installed. With this update, the source code of the **cockpit** RHEL system role was changed to use the **dnf** module directly with an

asterisk wildcard package name and a list of packages to exclude. As a result, the role correctly installs all requested packages that match the wildcard pattern.

Jira:RHEL-45944[1]

8.7. SUPPORTABILITY

The **sos clean** on an existing archive no longer fails

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

Jira:RHEL-35945

The sos stops collecting user's **.ssh** configuration

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

Jira:RHEL-22389

8.8. CONTAINERS

Netavark no longer fails resolving DNS TCP queries

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

Jira:RHEL-52247

CHAPTER 9. TECHNOLOGY PREVIEW FEATURES

This part provides a list of all Technology Preview features available in Red Hat Enterprise Linux 10.

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

9.1. IDENTITY MANAGEMENT

HSM support is available as a Technology Preview

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

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

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

You need the following:

- A supported HSM

- The HSM PKCS #11 library

- An available slot, token, and the token password

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

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

Jira:RHELDOCS-17465[1]

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

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

Jira:RHELDOCS-18408[1]

9.2. VIRTUALIZATION

AMD SEV, SEV-ES, and SEV-SNP for KVM virtual machines are available as Technology Preview

As a Technology Preview, RHEL 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 VM security.

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 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 to 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. * SEV-SNP works only on 4rd generation AMD EPYC CPUs (codenamed Genoa) or later.

Also note that RHEL includes SEV, SEV-ES, and SEV-SNP encryption, but not the SEV, SEV-ES, and SEV-SNP security attestation and live migration.

Jira:RHELDOCS-16800[1]

9.3. CONTAINERS

composefs filesystem is available as a Technology Preview

The key technologies **composefs** uses are:

- OverlayFS as the kernel interface

- Enhanced Read-Only File System (EROFS) for a mountable metadata tree

- The **fs-verity** feature (optional) from the lower filesystem

Key advantages of **composefs**:

- Separation between metadata and data. **composefs** does not store any persistent data. The underlying metadata and data files are stored in a valid lower Linux filesystem such as **ext4**, **xfs**, **btrfs**, and so on.

- Mounting multiple **composefs** with a shared storage.

- Data files are shared in the page cache to enable multiple container images to share their memory.

- Support **fs-verity** validation of the content files.

Jira:RHEL-52238

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

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

Jira:RHEL-32266

CHAPTER 10. REMOVED FEATURES

All removed features were deprecated in earlier releases and are no longer supported. For information regarding functionality that is present in RHEL 9 but has been *removed* in RHEL 10, see Considerations in adopting RHEL 10.

10.1. INSTALLER AND IMAGE CREATION

auth or authconfig commands are removed

The **auth** or **authconfig** Kickstart commands which were deprecated in Red Hat Enterprise Linux 8, are removed now. As a replacement, use the **authselect** kickstart command.

Jira:RHELDOCS-18839[1]

The inst.xdriver and inst.usefbx options have been removed

The graphical system for the installation image switched from the Xorg server to a Wayland compositor. As a consequence, the **inst.xdriver** boot option has been removed. Wayland operates without relying on X drivers, making it incompatible with loading any such drivers. As a result, the **inst.xdriver** option is no longer applicable.

Additionally, the **inst.usefbx** boot option, previously used to load a generic framebuffer X driver, has also been removed.

Jira:RHELDOCS-18818[1]

The openstack image type has been deprecated from RHEL image builder

From the RHEL 10-beta onward, RHEL image builder will no longer support the Openstack image type. You can use the **.qcow2** image type to build Openstack images.

Jira:RHELDOCS-18736[1]

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

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

Jira:RHELDOCS-18492[1]

Removed inst.nompath, dmraid and nodmraid boot options

The **inst.nompath**, **dmraid** and **nodmraid** boot options have been removed now and are no longer available for use.

Jira:RHELDOCS-18485[1]

Removed automatic bug reporting system from Anaconda

The installer no longer supports automatically reporting problems to the Red Hat issue tracking system. You can collect the installation logs and report problems manually, as described in the troubleshooting section.

Jira:RHELDOCS-18426[1]

Removed a few options of the timezone Kickstart command

The following options of the **timezone** Kickstart command has been removed in Red Hat Enterprise Linux 10:

- **--isUtc**: Use the option **--utc** instead.

- **--ntpservers**: Use the option **--ntp-server** of the timesource kickstart command instead.

- **--nontp**: Use the option **--ntp-disable** of the **timesource** kickstart command instead.

Jira:RHELDOCS-18423[1]

Removed the --level parameter of the logging Kickstart command

The **--level** parameter of the logging kickstart command has been removed. It is no longer possible to set the level of logging of the installation process.

Jira:RHELDOCS-18417[1]

The support for %anaconda Kickstart command has been removed

The support for the deprecated %anaconda Kickstart command has been removed. You can use the kernel arguments and command line line options to update the configuration in the **Anaconda configuration files**.

Jira:RHELDOCS-18416[1]

Removed pwpolicy Kickstart command

The support for the deprecated **pwpolicy** Kickstart command has been removed in Red Hat Enterprise Linux 10.

Jira:RHELDOCS-18415[1]

Removed support for adding additional repositories from GUI

Previously, when configuring the installation source, you could configure the additional repositories for the package installation. Starting in RHEL 10, this support has been removed. However, you can use the Kickstart installation method or **inst.addrepo** boot option if you want to specify additional repositories.

Jira:RHELDOCS-18413[1]

Removed support of the LUKS version selection from Anaconda

Previously, you could select the LUKS version from the Manual Installation screen. Starting in RHEL 10, the installer uses the **luks2** version by default for all the new devices. No changes are made to the existing devices' LUKS version. You can also use the Kickstart method to select different LUKS versions.

Jira:RHELDOCS-18412[1]

The initial-setup package now has been removed

The initial-setup package has been removed in Red Hat Enterprise Linux 10. As a replacement, use **gnome-initial-setup** for the graphical user interface.

Jira:RHELDOCS-18411[1]

Redesigned the Time & Date spoke in the Installer GUI

Previously, Anaconda users were able to select the timezone using the time zone map. This screen is now redesigned and the timezone map has been replaced with the options where users can set the required timezone.

For more information, refer to the installation documentation.

Jira:RHELDOCS-18410[1]

Removed teaming options from the **network** kickstart command

The **--teamslaves** and **--teamconfig** options used for configuring team devices in the **network** kickstart command have been removed. To configure similar network settings, use the **--bondslaves** and **--bondopts** options to set up a **Bond** device.

Jira:RHEL-33892

Removed NVDIMM reconfiguration support during the installation process

The support for reconfiguring NVDIMM devices during the Kickstart and GUI installation has been removed in RHEL-10. However, the NVDIMM devices in the sector mode can still be usable in the installation program.

Jira:RHELDOCS-19084

The **--excludeWeakdeps** and **--instLangs** options from **%packages** have been removed

In RHEL-10, the **--excludeWeakdeps** and **--instLangs** options used in the **%packages** section have been removed. To maintain similar functionality, use the updated options **--exclude-weakdeps** and **--inst-langs** instead. These replacements ensure compatibility and provide the same dependency and language control within package management.

Jira:RHELDOCS-19083

10.2. SECURITY

scap-workbench is removed

The **scap-workbench** package is removed in RHEL 10. 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-19009[1]

oscap-anaconda-addon is removed

The **oscap-anaconda-addon**, which provided means to deploy baseline-compliant RHEL systems by using the graphical installation, is removed in RHEL 10. 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-19010[1]

OVAL removed from vulnerability scanning applications

The Open Vulnerability Assessment Language (OVAL) data format, which provides declarative security data processed by the OpenSCAP suite, has been removed. Red Hat continues to provide declarative security data in the Common Security Advisory Framework (CSAF) format, which is the successor of OVAL.

Jira:RHELDOCS-19071[1]

DSA and SEED algorithms have been removed from 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 removed from the Network Security Services (NSS) cryptographic library. You can instead use algorithms such as RSA and ECDSA.

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

Jira:RHEL-44995

/etc/system-fips removed

Support for indicating FIPS mode through the **/etc/system-fips** file has been removed from 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:RHELDOCS-19357[1]

HeartBeat removed from TLS

The support for the HeartBeat extension in TLS has been removed to reduce the attack surface.

Jira:RHEL-59212[1]

SRP authentication removed from TLS

Authentication that uses Secure Remote Password protocol (SRP) in TLS has been removed from the **gnutls** package and is no longer supported. SRP authentication is considered insecure because it cannot be used with TLS 1.3 and relies on Cipher block chaining (CBC) and SHA-1 as a key exchange.

Jira:RHEL-58640[1]

Keylime no longer supports HTTP for revocation notifications

The Keylime components no longer support the HTTP protocol for revocation notification webhooks. Use HTTPS instead. 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-51279

DEFAULT cryptographic policy rejects TLS ciphers with RSA key exchange

TLS ciphers that use the RSA key exchange are no longer accepted in the **DEFAULT** system-wide cryptographic policy in RHEL 10. These ciphers do not provide perfect forward secrecy and are not considered as secure as ciphers that use other key exchanges, for example, the Elliptic-curve Diffie-Hellman (ECDH) key exchange.

This change also reduces the exposure to side-channel attacks because the RSA key exchange uses PKCS #1 v1.5 encryption padding, which can cause vulnerability to timing side-channel attacks.

If you need the RSA key exchange for interoperability with legacy systems, you can re-enable it by using the LEGACY system-wide cryptographic policy or by applying a custom subpolicy.

Jira:RHEL-50464[1]

ca-certificates trust store moved

The **/etc/pki/tls/certs** trust store is converted to a different format better optimized for OpenSSL. As a consequence, if you use the files in **/etc/pki/tls/certs** directly, switch to the **/etc/pki/ca-trust/extracted** directory, where the same data is stored. For example, software that accesses the trust bundle at **/etc/pki/tls/certs/ca-bundle.crt** should switch to using **/etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem** instead.

Jira:RHEL-50293

The **LEGACY** cryptographic policy disallows SHA-1 signatures in TLS

The **LEGACY** system-wide cryptographic policy in RHEL 10 no longer allows creating or verifying signatures that use SHA-1 in TLS contexts. Therefore, libraries other than OpenSSL might no longer accept or create any signatures that use SHA-1 regardless of use case. OpenSSL continues to accept signatures that use SHA-1 when not used for TLS if the system is in **LEGACY** or this functionality is re-enabled with a custom subpolicy.

Jira:RHEL-50106

pam_ssh_agent_auth is removed

The **pam_ssh_agent_auth** package has been removed from RHEL 10.

Jira:RHEL-45002

OpenSSL no longer permits SHA-1 at **SECLEVEL=2** in TLS

OpenSSL does not accept the SHA-1 algorithm at **SECLEVEL=2** in TLS in RHEL 10. If your scenario requires using TLS 1.0/1.1, you must explicitly set **SECLEVEL=0** and switch to the LEGACY system-wide cryptographic policy. In the LEGACY policy, applications that use SHA-1 in signatures outside of TLS will continue to work.

Jira:RHEL-39962

stunnel does not support OpenSSL ENGINE API

The **stunnel** TLS offloading and load-balancing proxy no longer supports the previously deprecated OpenSSL ENGINE API. The most common use case was accessing hardware security tokens by using PKCS #11 through the **openssl-pkcs11** package. As a replacement, you can use the **pkcs11-provider**, which uses the new OpenSSL provider API.

Jira:RHEL-33749

OpenSSL Engines removed from OpenSSL

OpenSSL Engines have been deprecated and will soon be removed from upstream. Therefore, the **openssl-pkcs11** package has been removed from OpenSSL in RHEL 10. Use providers instead, such as the **pkcs11-provider**, which is supported in this version.

Jira:RHEL-30437

10.3. SUBSCRIPTION MANAGEMENT

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

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 previously deprecated modules have been removed:

- **addons**

- **attach**

- **auto-attach**

- **import**

- **remove**

- **redeem**

- **role**

- **service-level**

- **usage**

- **syspurpose addons**

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

Jira:RHELDOCS-18989[1]

10.4. SOFTWARE MANAGEMENT

The support for the **libreport** library has been removed

The support for the **libreport** library has been removed from DNF. If you want to attach DNF logs to your bug reports, you need to do it manually or by using a different mechanism.

Jira:RHEL-40382

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

The DNF **debug** plug-in, which included the **dnf debug-dump** and **dnf debug-restore** commands, has been removed from the **dnf-plugins-core** package. Depending on your scenario, you can use one of the following commands instead:

- **dnf list --installed** or **dnf repoquery --installed** to list packages installed on your system.

- **dnf repolist -v** to list repositories enabled on your system.

- **dnf install $(</tmp/list)** to replicate packages installed on a source system to the target system. For example:

  1. Save a list of packages installed on a source system into the **/tmp/list** file:

```
$ dnf repoquery --installed >/tmp/list
```

2. Copy the **/tmp/list** file to the target system.

3. Replicate packages on the target system:

```
$ dnf install $(</tmp/list)"
```

Jira:RHEL-23706[1]

10.5. INFRASTRUCTURE SERVICES

Significant changes in the package set for infrastructure services

The following packages are no longer included in Red Hat Enterprise Linux:

- **sendmail** : Red Hat recommends migrating to the postfix mail daemon, that is supported.

- **redis** : Red Hat recommends migrating to the **valkey** package.

- **dhcp** : Red Hat recommends migrating to the available alternatives such as **dhcpcd** and **ISC Kea**.

- **mod_security**: The **mod_security** directive is now available in the EPEL repository.

- **spamassassin** : The Spamassassin mail filter is now available in the EPEL repository instead of the standard RHEL repository as it depends on the **libdb** (Berkeley DB) library, which is unavailable due to licensing issues.

- **xsane** : The API is not yet ported to **Gtk3**.

The following packages have been renamed:

- **gpsd** : It was previously included as **gpsd-minimal**.

Jira:RHEL-22424[1]

10.6. NETWORKING

The **dhcp-client** package has been removed

The **dhcp-client** package has been removed from RHEL 10, because the ISC DHCP client is no longer maintained upstream. As a consequence, the **dhclient** utility is no longer available and you cannot use it as DHCP client in NetworkManager. As an alternative, use the NetworkManager-internal DHCP client, which was also the default in previous RHEL versions.

Jira:RHEL-46211

The **mlx4** driver is removed from RHEL 10.0-Beta

With the RHEL 10.0-Beta release, the **mlx4** driver for the Mellanox ConnectX-3 network interface controller (NIC) is removed. You must use another NIC that is compatible with newer drivers.

Jira:RHEL-40070

10.7. KERNEL

The **kexec_load** system call is removed

The kexec_load system call, which was deprecated in RHEL 9, is removed. In RHEL 10, the kexec_file_load system call replaces kexec_load and is the default system call on all architectures. Also, kexec_file_load is required for a secure boot.

For more information, see Is kexec_load supported in RHEL9?

Jira:RHEL-29272[1]

10.8. FILE SYSTEMS AND STORAGE

Support for NVMe devices has been removed from the **lsscsi** package

Support for Non-volatile Memory Express (NVMe) devices has been removed from the **lsscsi** package. Use native tools such as **nvme-cli**, **lsblk**, and **blkid** instead. Report any missing functionality against the **nvme-cli** package.

Jira:RHEL-32144[1]

Support for NVMe devices has been removed from the **sg3_utils** package

Support for Non-volatile Memory Express (NVMe) devices has been removed from the **sg3_utils** package. Use native tools such as the **nvme-cli** package instead and report any missing functionality against **nvme-cli**.

Jira:RHEL-412[1]

The VDO **sysfs** parameters have been removed

The Virtual Data Optimizer (VDO) **sysfs** parameters have been removed. Except for **log_level**, all module-level **sysfs** parameters for the **kvdo** module are removed. For individual **dm-vdo** targets, all **sysfs** parameters specific to VDO are also removed. There is no change for the parameters that are common to all DM targets. Configuration values for **dm-vdo** targets that 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:RHELDOCS-19066[1]

Support for GFS2 file systems has been removed

The Red Hat Enterprise Linux (RHEL) Resilient Storage Add-On will no longer be supported starting with Red Hat Enterprise Linux 10. This includes the GFS2 file system, which is also no longer supported. 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-19024[1]

10.9. HIGH AVAILABILITY AND CLUSTERS

pcsd Web UI no longer available as a standalone user interface

The **pcsd** Web UI has been modified to be usable as a RHEL web console add-on and is no longer operated as a standalone interface.

Jira:RHEL-29739

Removed functionality for the Red Hat High Availability Add-On

The following Red Hat High Availability Add-On features are no longer supported in RHEL 10.

- Using spaces in dates in location constraint rules

- Delimiting stonith devices with a comma in **pcs stonith level add | clear | delete | remove** commands

- Ambiguous syntax of the **pcs stonith level clear | delete | remove** command. The command has been clarified to distinguish a target from a stonith device.

- The legacy role names of **master** and **slave** are no longer accepted by the **pcs** command-line interface. Use **Promoted**, **Unpromoted**, --promoted, **promotable**, and **promoted-max** instead.

- Using stonith resources in **pcs resource** commands and resources in **pcs stonith** commands, as well as **--brief**, **--no-strict,--safe** and **--simulate** flags of the **pcs stonith disable** command

- Ability to create a stonith resource in a group with the **pcs stonith create** command

- The **stonith.create_in_group** command from API v1 and v2

- The **pcs cluster pcsd-status** command. Use the **pcs status pcsd** or **pcs pcsd status** command.

- The **pcs cluster certkey** command. Use the **pcs pcsd certkey** command.

- The **pcs resource | stonith [op] defaults <name>=<value>…** command. Use the **pcs resource | stonith [op] defaults update** command.

- The **pcs acl show** command. Use the **pcs acl config** command.

- The **pcs alert show** command. Use the **pcs alert config** command.

- The **pcs constraint [location | colocation | order | ticket] show | list** commands. Use the **pcs constraint [location | colocation | order | ticket] config** command.

- The **pcs property show** and the **pcs property list** commands. Use the **pcs property config** command.

- The **pcs tag list** command. Use the **pcs tag config** command.

- The **--autodelete** flag of the **pcs resource move** command.

Jira:RHEL-34783

Support for the RHEL Resilient Storage Add-On has been removed

The Red Hat Enterprise Linux (RHEL) 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-19023[1]

10.10. COMPILERS AND DEVELOPMENT TOOLS

32-bit packages have been removed in RHEL 10

Linking against 32-bit multilib packages has been removed. The ***.i686** packages remain supported for the life cycle of Red Hat Enterprise Linux 9.

Jira:RHELDOCS-19269

10.11. IDENTITY MANAGEMENT

The **pam_console** module has been removed

The **pam_console** module has been removed from RHEL 10. The **pam_console** module granted file permissions and authentication capabilities to users logged in at the physical console or terminals, and adjusted 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-18159[1]

The NIS server emulator has been removed

RHEL Identity Management (IdM) does not provide the NIS functionality anymore.

Jira:RHEL-34186

Other removed functionality for RHEL Identity Management

The following packages were part of RHEL 9 but are not distributed with RHEL 10:

- **compat-hesiod**

- **fontawesome-fonts**: consider using **fontawesome4-fonts** instead

- **libnsl2**

- **python3-netifaces**: consider using using **python-ifaddr** instead

Jira:RHEL-33818

BDB is no longer supported in **389-ds-base**

The **libdb** library that implements the Berkeley Database (BDB) version used by **389-ds-base** is no longer available in RHEL 10. As a result, Directory Server no longer supports BDB.

As a replacement, Directory Server creates instances with Lightning Memory-Mapped Database (LMDB).

Jira:RHEL-30640

10.12. SSSD

The **enumeration** feature has been removed for AD and IdM

Support for the **enumeration** feature was deprecated for AD and IdM in Red Hat Enterprise Linux (RHEL) 9. The **enumeration** feature has been removed for AD and IdM in RHEL 10.

Jira:RHELDOCS-19005

The libsss_simpleifp subpackage has been removed

The **libsss_simpleifp** subpackage that provided the **libsss_simpleifp.so** library was deprecated in Red Hat Enterprise Linux (RHEL) 9. The **libsss_simpleifp** subpackage has been removed in RHEL 10.

Jira:RHELDOCS-19094

The SSSD files provider has been removed

The SSSD files provider has been removed from RHEL 10.0. Previously, the SSSD files provider was responsible for smart card authentication and session recording for local users. As a replacement, you can configure the SSSD proxy provider.

Due to the removal of the files provider, the **authselect minimal** profile has been replaced by a new **local** profile.

Jira:RHELDOCS-19267[1]

10.13. DESKTOP

TigerVNC has been removed

The TigerVNC remote desktop solution has been removed in RHEL 10.

TigerVNC provided the server and client implementation of the Virtual Network Computing (VNC) protocol in RHEL 9.

The following packages have been removed:

- **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. TigerVNC is replaced by the **gnome-remote-desktop** daemon, which is a remote desktop server that uses the RDP protocol. You can use the **gnome-remote-desktop** in the following modes:

- Desktop sharing: provides sharing of your physical session by using Assisted Access

- Headless session: provides a single user remote headless session

- Remote login: provides a graphical remote login and replaces functionality of XDMCP

Jira:RHELDOCS-18388[1]

Totem media player has been removed in RHEL 10

The RHEL 10 installation does not contain any media player by default. You can use any third party media player available, for example, on Flathub.

Jira:RHELDOCS-18389[1]

power-profiles-daemon is removed in RHEL 10

The **power-profiles-daemon** package that provided power mode configuration in GNOME has been removed in RHEL 10. In RHEL 10, you can manage power profiles with the Tuned daemon.

The **tuned-ppd** package provides a drop-in replacement for **power-profiles-daemon**, which allows it to be used with GNOME desktop and applications that use **power-profiles-daemon** API. You can also use it to override the three basic power profiles, including **power-saver**, **balanced**, and **performance** through the **/etc/tuned/ppd.conf** configuration file. If you want to use a customized profile, you can edit the configuration file and map the custom profile to the three basic **power-profiles-daemon** profile names.

Jira:RHELDOCS-18390[1]

gedit is removed in RHEL 10

gedit, the default graphical text editor in Red Hat Enterprise Linux, is removed in RHEL 10. As an alternative, you can use GNOME Text Editor.

Jira:RHELDOCS-19148[1]

Tweaks is no longer available as a RHEL package in RHEL 10

Instead of the Tweaks desktop application, you can use the default GNOME Settings app, which has been expanded to include many options previously only found in Tweaks.

Jira:RHELDOCS-19125[1]

Qt5 libraries are removed in RHEL 10

Qt5 libraries are replaced with Qt6 libraries, with new functionality and better support.

For more information, see Porting to Qt 6 .

Jira:RHELDOCS-19132[1]

WebKitGTK is removed in RHEL 10

The WebKitGTK web browser engine is removed in RHEL 10. As a consequence, you can no longer 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-19170[1]

Evolution is removed in RHEL 10

Evolution is a GNOME application that provides integrated email, calendar, contact management, and communications functionality. The application and its plugins are removed in RHEL 10. You can find an alternative in a third party source, for example on Flathub.

You can back up your Evolution data directly in Evolution using the **Back up Evolution data** item in the **File** menu.

Jira:RHELDOCS-19146[1]

Festival is not supported in RHEL 10

With support for the Festival speech synthesizer removed in RHEL 10, the Festival binaries, libraries and the plugin for Speech Dispatcher are also removed.

As an alternative, you can use the Espeak NG speech synthesizer.

Jira:RHELDOCS-19138[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-19134[1]

Cheese is removed

The Cheese camera application is removed in RHEL 10.

As an alternative, you can use the Snapshot application.

Jira:RHELDOCS-19136[1]

Devhelp has been removed

Devhelp, a graphical developer tool for browsing and searching API documentation, has been removed in RHEL 10. You can now find API documentation online in specific upstream projects.

Jira:RHELDOCS-19153[1]

gtkmm based on GTK 3 has been removed

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

Jira:RHELDOCS-19142[1]

LibreOffice is removed in RHEL 10

The LibreOffice RPM packages are removed from RHEL 10. 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: link:https://flathub.org/apps/org.libreoffice.LibreOffice. The official RPM packages: link:https://www.libreoffice.org/download/download-libreoffice/.

Jira:RHELDOCS-19152[1]

GNOME Terminal is removed in RHEL 10

GNOME Terminal has been replaced with Ptyxis in RHEL 10.

Ptyxis is a container-oriented terminal that provides transparent support for container systems like Podman or Toolbx and robust support for user profiles.

Jira:RHELDOCS-19155[1]

Inkscape vector graphics editor is removed in RHEL 10

The RHEL 10 installation does not contain any vector graphics editor. You can use any third party vector graphics editor available, for example, on Flathub.

Jira:RHELDOCS-19150[1]

10.14. GRAPHICS INFRASTRUCTURES

The PulseAudio daemon is removed in RHEL 10

The PulseAudio daemon, and its packages **pulseaudio** and **alsa-plugins-pulseaudio**, have been removed in RHEL 10.

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-17682[1]

Motif is removed

Motif is an X11-based Desktop Environment (DE), which consists of a toolkit and the **mwm** X11 window manager. It was previously deprecated and has been removed from RHEL 10. As a replacement, you can use the GTK or Qt toolkit.

Jira:RHELDOCS-19221[1]

xorg-x11-server is removed from RHEL 10

The X.Org server, an implementation of the X Window System, was previously deprecated and is removed from RHEL 10. Note that the X11 protocol is not removed, which means that most applications will remain compatible through the Xwayland compositor. For more information, see Red Hat Enterprise Linux 10 plans for Wayland and Xorg server (Red Hat Blog).

Jira:RHELDOCS-19222[1]

10.15. VIRTUALIZATION

The virt-v2v tool can no longer convert Xen virtual machines from RHEL 5

It is no longer possible to use the **virt-v2v** tool to convert virtual machines from a RHEL 5 Xen host to KVM. For details, see the Red Hat Knowledge Base.

Jira:RHEL-37687

Red Hat Virtualization compatibility has been removed from virt-v2v

Because the maintenance support for Red Hat Virtualization (RHV) has ended, the **virt-v2v** utility no longer supports exporting virtual machines to RHV. As a consequence, the following options are no longer available in **virt-v2v**:

- **-o rhv-upload**

- **-o rhv**

- **-o vdsm**

Jira:RHEL-36712

10.16. RHEL IN CLOUD ENVIRONMENTS

cloud-init no longer uses python-jsonschema

This update has removed the **cloud-init** dependency on the **python-jsonschema** package. As a consequence, it is no longer possible use the **cloud-init** schema validator to verify **cloud-init** configuration.

Jira:RHEL-65849[1]

CHAPTER 11. DEPRECATED FEATURES

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

Features can be deprecated during a major version's release cycle.

A deprecated feature is listed in all future release notes until it is removed. For a complete list of deprecated features, see the release notes for the latest minor version. For information about the length of support, see Red Hat Enterprise Linux Life Cycle and Red Hat Enterprise Linux Application Streams Life Cycle.

11.1. INSTALLER AND IMAGE CREATION

Anaconda built-in help has been removed

The built-in documentation from spokes and hubs of all Anaconda user interfaces, which was available during Anaconda installation, has been removed. Instead, refer to the official RHEL documentation.

Jira:RHELDOCS-18414[1]

The **squashfs** package has been deprecated

The **squashfs** package has been deprecated, and. As an alternative, **dracut** has support for mounting **erofs**.

Jira:RHELDOCS-18903[1]

sgdisk has been deprecated from the **boot.iso**

gdisk has been deprecated from the **boot.iso** image type. You still can use **gdisk** in your kickstarts. For the **boot.iso** image type, other tools are available for handling GPT disks, for example, the **parted** utility.

Jira:RHELDOCS-18904[1]

The module kickstart command has been deprecated

Anaconda has deprecated its support for DNF modularity, and as a consequence the **module** kickstart command has been deprecated. This might impact you if you are using modules in the **%packages** section of your kickstart files or the **module** kickstart command. This change is implemented for simplifying the installation process and ensuring a more consistent experience moving forward.

Jira:RHEL-34829

The **inst.gpt** boot option is now deprecated

The **inst.gpt** boot option is now deprecated and will be removed in the future releases. To specify a preferred disk label type, use the **inst.disklabel** boot option. Specify **gpt** or **mbr** to create GPT or MBR disk labels, respectively.

Jira:RHELDOCS-18491[1]

11.2. SECURITY

ENGINE API in OpenSSL is deprecated

In RHEL 10, ENGINE API is deprecated and is planned to be removed in a future major release. No new applications should be built by using the ENGINE API. To keep application binary interface (ABI) and existing applications working, OpenSSL still exports the ENGINE symbols. To prevent new applications from using ENGINE API, OpenSSL sets the **OPENSSL_NO_ENGINE** flag system-wide, and the header **engine.h** that exposes the ENGINE API has been removed.

Jira:RHEL-45704

HMAC-SHA-1 in FIPS mode is deprecated

The HMAC-SHA-1 cryptographic algorithm is deprecated in FIPS mode, and it may be removed in a future release. Outside FIPS mode, support for HMAC-SHA-1 is preserved.

Jira:RHELDOCS-18674

11.3. SHELLS AND COMMAND-LINE TOOLS

The **perl(Mail::Sender)** module has been removed

The **perl(Mail::Sender)** module is removed from RHEL 10 without any replacement. As a consequence, 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:RHEL-44478[1]

11.4. HIGH AVAILABILITY AND CLUSTERS

Deprecated High Availability Add-On features

The following features have been deprecated in Red Hat Enterprise Linux 10 and will be removed in the next major release

- Specifying rules as multiple arguments. Use a single string argument instead.

- Specifying **score** as a standalone value in **pcs constraint location add** and **pcs constraint colocation ad**. Use **score=value** instead.

- Specifying the **--wait** option in resource commands except **pcs resource restart | move**, and in the commands **pcs cluster node add-guest | add-remote**. Use the following commands instead:

  - **pcs status wait** to wait for the cluster to settle into stable state.

  - **pcs status query resource** commands to verify that the resource is in the expected state after the wait.

- Using the **--force** flag to confirm potentially destructive actions such as **pcs cluster destroy**, **pcs quorum unblock**, **pcs stonith confirm**, **pcs stonith sbd device setup**, and **pcs stonith sbd watchdog test** commands. You should now use the **--yes** flag to confirm potentially destructive actions and reserve use of the **--force** flag to override validation errors.

- Using the **--force** flag to confirm overwriting files in **pcs cluster report**. Use the **--overwrite** flag instead.

- Assigning and unassigning ACL roles without specifying the **user** or **group** keyword.

The **pcs** command-line interface produces a warning when a user attempts to configure a system with these deprecated 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:RHELDOCS-18544[1]

11.5. COMPILERS AND DEVELOPMENT TOOLS

The `utmp` and `utmpx` interfaces in `glibc` are deprecated

The **utmp** and **utmpx** interfaces provided by the **glibc** library include a counter that counts time since the Unix epoch. This counter will overflow on February 07, 2106. Therefore, **utmp** and **utmpx** are deprecated in RHEL 10 and will be removed in RHEL 11.

Jira:RHELDOCS-18080[1]

11.6. THE WEB CONSOLE

The host switcher in the RHEL web console is deprecated

The host switcher that provides connections to multiple machines through SSH from a single RHEL web console session is deprecated and disabled by default. Due to the web technology limitations, this feature cannot be secure. You can enable the host switcher after assessing the risks in your scenario. As more secure alternatives, you can use:

- the web console login page (with the secure limit of one host in a web browser session)

- the Cockpit Client flatpack

Jira:RHEL-4032[1]

11.7. VIRTUALIZATION

libslirp has been deprecated

In RHEL 10, the **libslirp** networking back end has become deprecated, and will be removed in a future major version release.

Jira:RHEL-45147

The i440fx virtual machine type has been deprecated

In RHEL 10, the **i440fx** machine types for virtual machines (VMs) have become deprecated, and will be removed in a future major version of RHEL.

In addition, the **i440fx-rhel7.6** machine type has been replaced by **i440fx-rhel10.0**. As a consequence, a VM with a **i440fx-rhel7.6** machine type will not boot correctly after live migrating to a RHEL 10 host. To work around this issue, restart the VM after live migration.

Jira:RHELDOCS-18672[1]

11.8. CONTAINERS

The `runc` container runtime has been removed

The **runc** container runtime is removed. The default container runtime is **crun**. If you upgrade from the previous RHEL versions to RHEL 10.0 Beta, you have to run the **podman system migrate --new-runtime=crun** command to set a new OCI runtime for all containers.

Jira:RHELDOCS-19051[1]

tzdata package is no longer installed by default in the minimal container images

The **tzdata** package is no longer installed in the **registry.access.redhat.com/ubi10-beta-minimal** container image. As a consequence, if you migrate your minimal container builds from a previous RHEL release to RHEL 10.0 Beta, and you enter the **microdnf reinstall tzdata** command to reinstall the **tzdata** package, you get an error message because the **tzdata** package is no longer installed by default. In this case, enter the **microdnf install tzdata** command to install **tzdata**.

Jira:RHELDOCS-18700[1]

The Podman v5.0 deprecations

In RHEL 10.0 Beta, 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 **containernetworking-plugins** package and the CNI network stack are no longer supported.

  - If you upgrade from the previous RHEL versions to RHEL 10.0 Beta or if you have a fresh installation of RHEL 10.0 Beta, the CNI is no longer available. As a result, you have to run the **podman rmi --all --force** command to remove all images and containers that are using those images.

  - If present, the **cni** value in the containers.conf file for the **network_backend** option must be changed to **netavark** or can be unset.

Jira:RHEL-40641

11.9. 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.
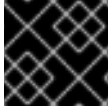
> **IMPORTANT**
>
> The support status of deprecated packages remains unchanged within RHEL 10.

The following packages have been deprecated in RHEL 10:

- daxio

- gvisor-tap-vsock-gvforwarder

- libpmem

- libpmem2

- libpmemblk

- libpmemlog

- libpmemobj

- libpmemobj-cpp

- libpmempool

- libslirp

- nvml

- pmempool

- pmreorder

- wget

CHAPTER 12. KNOWN ISSUES

This version of Red Hat Enterprise Linux 10.0 Beta is affected by the following newly identified and previously known issues. A known issue is listed in all future release notes until resolved, at which point it is published as a fixed issue. If you encountered an issue that is not listed in this section, please report it by using the button in the top right corner of this page.

12.1. INSTALLER AND IMAGE CREATION

Anaconda installer appears as unresponsive in the rescue mode

When booting into a rescue mode and selecting the **Continue** or **Skip to shell** options, you might experience an issue where the Anaconda installer appears to be frozen. Despite the lack of visible response, the installer is still functional and reacting to your inputs; however, the prompt does not display on the screen, leading to confusion.

Continue with your tasks as normal, as the installer is still operational despite the absence of a visible prompt.

Jira:RHEL-58834[1]

Unable to register RHEL-10 beta systems with Red Hat Satellite

Currently, Red Hat Satellite does not support RHEL-10 clients. As a result, attempting to register your system to a Satellite instance during the RHEL-10 beta installation fails. As a consequence, your system remains unregistered to Satellite after installation, which might impact further system management through Satellite. At the moment, there is no workaround.

Jira:RHELDOCS-18815[1]

Unable to build ISOs from a signed container

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

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

This happens because the system fails to get the image source signatures. To work around this issue, you can either remove the signature from the container image or build a derived container image. For example, to remove the signature, you can run the following command:

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

```
quay.io/centos-bootc/bootc-image-builder \
--type iso --local \
registry.redhat.io/rhel9-beta/rhel-bootc:9.4
```

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

Jira:RHEL-34807

12.2. SUBSCRIPTION MANAGEMENT

The Red Hat Insights remediations service is not available to execute playbooks in RHEL 10-beta for directly connected systems

Due to a missing RPM package (**rhc-worker-playbook**), the remediations service cannot execute playbooks in RHEL 10-beta for systems that are directly connected with the remote host configuration (**rhc**) client.

There is currently no workaround for this known issue in RHEL 10-beta.

Jira:RHELDOCS-18991

12.3. INFRASTRUCTURE SERVICES

Nginx does not support PKCS #11 and TPM

The OpenSSL engines API was deprecated in RHEL 9 and removed from Nginx in RHEL 10. The corresponding functionality using the current OpenSSL providers API is not yet available. As a consequence, the Nginx HTTP server does not work with hardware security modules (HSMs) through PKCS #11 and Trusted Platform Module (TPM) devices.

Jira:RHEL-33742

12.4. KERNEL

crashkernel boot parameter does not load in rhel-guest-image

Presently, RHEL cloud image built by **osbuild** misses the **crashkernel** kernel parameter. As a result, **kdump.service** fails to start.

To work around this issue, run **kdumpctl** manually to set up the **crashkernel** kernel parameter and reboot the system. **kdump.service** will start successfully.

Jira:RHEL-63071[1]

The kdump service fails during boot

After the installation of **registry.redhat.io/rhel9/rhel-bootc** container image to a physical system, the **kdump.service** fails.

To work around this problem, ensure the **PrivateTmp** service is disabled:

```
# cat /etc/systemd/system/kdump.service.d/override.conf
[Service]
PrivateTmp=no
```

Then rebuild and restart the kdump service:

```
# touch /etc/kdump.conf
# systemctl restart kdump
```

Jira:RHEL-50736

12.5. COMPILERS AND DEVELOPMENT TOOLS

The new version of TBB is incompatible

RHEL 10 includes the Threading Building Blocks (TBB) library version 2021.11.0, which is incompatible with the versions distributed with previous releases of RHEL. You must rebuild applications that use TBB to make them run on RHEL 10.

Jira:RHEL-33633

12.6. IDENTITY MANAGEMENT

The IdM server functions only partially or not at all

In this release, changes introduced by OpenSSL have impacted the integrated DNS functionality within Identity Management (IdM). Most notably, the OpenSSL PKCS #11 engine is replaced by a new **pkcs11-provider**. This shift affects multiple components in IdM, including **ipa**, **bind**, **bind-dyndb-ldap**, **softhsm**, and **python-cryptography**.

The transition from the **openssl-pkcs11** engine to the **pkcs11-provider** changes the way these components interact with security modules. As a result, all IdM components relying on the previous OpenSSL engine require updates to remain compatible with the new **pkcs11-provider**.

To support the new **pkcs11-provider**, a migration to Bind 9.20 is necessary. Bind 9.20 is the first version that provides compatibility with the **pkcs11-provider**, but it also introduces substantial architectural changes. These changes require a major rewrite of the **bind-dyndb-ldap** plugin to ensure that it continues functioning properly with the updated Bind and OpenSSL configurations.

Consequently, the IdM server functions only partially or not at all in RHEL 10-Beta. Specifically, you cannot install the **ipa-server-dns** package, and the embedded DNS server cannot be configured using the **--setup-dns** option. Until the necessary updates to **bind-dyndb-ldap** and other impacted components are completed, the integrated DNS feature remains unavailable.

Jira:RHEL-30556

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]

Migrating an IdM deployment may result in duplicate HBAC rules

Migrating from one Identity Management (IdM) deployment to another by using the **ipa-migrate** utility may lead to duplicate host-based access control (HBAC) rules on the destination server. Consequently,

the **allow_all** and **allow_systemd-user** HBAC rules appear twice when running the **ipa hbacrule-find** command on that server.

To work around the problem:

1. Identify the distinguished name of the duplicate HBAC rule by using the **ipa hbacrule-find --all --raw** command.

2. Delete the duplicate rule by using the **ldapdelete** command.

Jira:RHEL-59265[1]

Installing a RHEL 7 IdM client with a RHEL 10 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 10 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 10 fails.

To work around the problem, upgrade the host to RHEL 8 or later before installing an IdM client on it.

Jira:RHELDOCS-19015[1]

Automatic host keytab renewal via **adcli** run by SSSD is failing

In direct SSSD-AD integration, SSSD checks daily if the machine account password is older than the configured age in days and, if needed, tries to renew it. The configured age is set by the **ad_maximum_machine_account_password_age** value, with a default of **30** days. A value of **0** disables the renewal attempt.

However, currently there is an issue and the automatic renewal of the machine account password fails. If the password expires, this may result in the host losing access to the AD domain.

Workaround: Renew the password manually or via another means. Do not rely on the SSSD automatic renewal.

Jira:RHELDOCS-19172[1]

dsctl healthcheck can report a wrong database type

If you created an instance with the Lightning Memory-Mapped Database Manager (LMDB) database type, running the **dsctl healthcheck** command can result in on of the following error messages, because Directory Server checks a wrong configuration parameter:

- **DSBLE0005**. Backend configuration attributes mismatch.

- **DSBLE0006**. BDB is still used as a backend.

To work around this issue, set the **NSSLAPD_DB_LIB** environment variable to **mdb** before running **dsctl healthcheck**.

Jira:RHELDOCS-19014[1]

An error message is displayed during migration from BDB to LMDB

When you run the **dsctl dblib bdb2mdb** command to migrate from Berkeley Database (BDB) to Lightning Memory-Mapped Database Manager (LMDB) and you have not enabled the replication, the following error message is displayed in the output:

> Error: 97 - 1 - 53 - Server is unwilling to perform - [] - Unauthenticated binds are not allowed

Note that you can ignore the error message. The error occurs because Directory Server attempts to find the **replication_changelog.db** file that is not mandatory when the replication is disabled. This error does not prevent the migration from BDB to LMDB.

There is currently no workaround for this issue.

Jira:RHELDOCS-19016[1]

Installing an IdM replica fails in FIPS mode

In RHEL 10-beta, the installation of an Identity Management (IdM) replica fails in FIPS mode. The installation fails when the import of the Registration Authority (RA) key is attempted.

Jira:RHEL-58067[1]

12.7. THE WEB CONSOLE

VNC console in the RHEL web console does not work correctly on ARM64

Currently, when you import a virtual machine (VM) in the RHEL web console on ARM64 architecture and then you try to interact with it in the VNC console, the console does not react to your input.

Additionally, when you create a VM in the web console on ARM64 architecture, the VNC console does not display the last lines of your input.

Jira:RHEL-31993[1]

12.8. VIRTUALIZATION

Using SEV-SNP is not possible

Currently, when attempting to start an AMD SEV-SNP enabled virtual machine (VM), QEMU checks the incorrect capability of KVM, and the guest fails to start. As a consequence, running VMs with AMD SEV-SNP configured is not possible with RHEL10 Beta. There is no workaround for the issue.

Jira:RHEL-58928[1]

IP address is not assigned to ARM64 Azure VMs at boot time

When you boot a RHEL-10.0-Beta VM with the ARM64 CPU on Microsoft Azure, no IP address is assigned to the VM. Consequently, you cannot access the VM through the network. As a workaround, follow the steps below to edit a **NetworkManager.conf** file:

```
# mkdir -p /etc/NetworkManager/conf.d
# cat > /etc/NetworkManager/conf.d/99-azure-unmanaged-devices.conf << EOF
# Ignore SR-IOV interface on Azure, since it's transparently bonded to the synthetic interface
[keyfile]
unmanaged-devices=driver:mlx4_core;driver:mlx5_core
EOF
```

After adding this configuration, if you enable single root I/O virtualization (SR-IOV), you can use Mellanox Virtual Function Network Interface Controller (VF NIC) to assign an IP to the VM.

Jira:RHEL-40417[1]

IP address assigned to VF NIC makes VMs inaccessible from external networks

When you boot a RHEL-10.0 beta VM with Microsoft Azure Network Adapter (MANA) on Microsoft Azure, an IP address gets assigned to the Virtual Function Network Interface Controller (VF NIC). As a consequence, the VM becomes inaccessible through the external network. As a workaround, add **driver:mana** to the **/etc/NetworkManager/conf.d/99-azure-unmanaged-devices.conf** file:

```
[keyfile]
unmanaged-devices=driver:mlx4_core;driver:mlx5_core;driver:mana
```

Jira:RHEL-50544[1]

12.9. RHEL IN CLOUD ENVIRONMENTS

RHEL 10 Beta guests in some cases terminate unexpectedly on GCP and Alibaba

When using a RHEL 10 Beta instance on Google Cloud Platform or the Alibaba Cloud, restarting the instance currently causes a kernel panic in the guest operating system if the **virtio-net** driver is in use. There is no known workaround.

Jira:RHEL-56981[1]

RDMA devices currently do not work on vSphere

When using a RHEL 10 instance on the VMware vSphere platform, the **vmw_pvrdma** module currently does not install properly. As a consequence, VMware paravirtual remote direct memory access (PVRDMA) devices do not work on the affected instances.

Jira:RHEL-41133[1]

12.10. CONTAINERS

Podman and bootc do not share the same registry login process

Podman and **bootc** use different registry login processes when pulling images. As a consequence, if you login to an image by using Podman, logging to a registry for **bootc** will not work on that image. When you install an image mode for RHEL system, and login to registry.redhat.io by using the following command:

```
# podman login registry.redhat.io <username_password>
```

And then you attempt to switch to the **registry.redhat.io/rhel9/rhel-bootc** image with the following command:

```
# bootc switch registry.redhat.io/rhel9/rhel-bootc:9.4
```

You should be able to see the following message:

```
Queued for next boot: registry.redhat.io/rhel9/rhel-bootc:9.4
```

However, an error appears:

> ERROR Switching: Pulling: Creating importer: Failed to invoke skopeo proxy method OpenImage: remote error: unable to retrieve auth token: invalid username/password: unauthorized: Please login to the Red Hat Registry using your Customer Portal credentials. Further instructions can be found here: https://access.redhat.com/RegistryAuthentication

To work around this issue, follow the steps Configuring container pull secrets to use authenticated registries with **bootc**.

Jira:RHELDOCS-18471[1]

cloud-init growpart skips with composefs is enabled

When composefs is enabled, if you generate an image from the generic base image, then the rootfs will note grow the filesystem, prompting an error similar to:

> 2024-04-30 17:27:53,543 - cc_growpart.py[DEBUG]: '/' SKIPPED: stat of 'overlay' failed: [Errno 2] No such file or directory: 'overlay'

As a workaround, you can add a custom growpart, by specifying the **rootfs** default size in the container, instead of dynamically choosing 100G at instance creation time to be able to write a partitioning config in the container.

Jira:RHEL-34859

12.11. KNOWN ISSUES IDENTIFIED IN PREVIOUS RELEASES

This part describes known issues in Red Hat Enterprise Linux 10.0 Beta.

12.11.1. Networking

Failure to update the session key causes the connection to break

Kernel Transport Layer Security (kTLS) protocol does not support updating the session key, which is used by the symmetric cipher. Consequently, the user cannot update the key, which causes a connection break. To work around this problem, disable kTLS. As a result, with the workaround, it is possible to successfully update the session key.

Bugzilla:2013650[1]

kTLS does not support offloading of TLS 1.3 to NICs

Kernel Transport Layer Security (kTLS) does not support offloading of TLS 1.3 to NICs. Consequently, software encryption is used with TLS 1.3 even when the NICs support TLS offload. To work around this problem, disable TLS 1.3 if offload is required. As a result, you can offload only TLS 1.2. When TLS 1.3 is in use, there is lower performance, since TLS 1.3 cannot be offloaded.

Bugzilla:2000616[1]

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-31780, Jira:RHEL-30640
NetworkManager	Jira:RHEL-1531, Jira:RHEL-46211
Release Notes	Jira:RHELDOCS-18787, Jira:RHELDOCS-19185, Jira:RHELDOCS-19191, Jira:RHELDOCS-17893, Jira:RHELDOCS-19162, Jira:RHELDOCS-19060, Jira:RHELDOCS-19059, Jira:RHELDOCS-19009, Jira:RHELDOCS-19010, Jira:RHELDOCS-19071, Jira:RHELDOCS-19357, Jira:RHELDOCS-19066, Jira:RHELDOCS-18389, Jira:RHELDOCS-18390, Jira:RHELDOCS-19148, Jira:RHELDOCS-19125, Jira:RHELDOCS-19132, Jira:RHELDOCS-19170, Jira:RHELDOCS-19146, Jira:RHELDOCS-19138, Jira:RHELDOCS-19134, Jira:RHELDOCS-19136, Jira:RHELDOCS-19153, Jira:RHELDOCS-19142, Jira:RHELDOCS-19152, Jira:RHELDOCS-19155, Jira:RHELDOCS-19150, Jira:RHELDOCS-17682, Jira:RHELDOCS-19221, Jira:RHELDOCS-19222, Jira:RHELDOCS-19023, Jira:RHELDOCS-19024, Jira:RHELDOCS-19094, Jira:RHELDOCS-18839, Jira:RHELDOCS-18492, Jira:RHELDOCS-18485, Jira:RHELDOCS-18414, Jira:RHELDOCS-18159, Jira:RHELDOCS-19051, Jira:RHELDOCS-18989, Jira:RHELDOCS-19084, Jira:RHELDOCS-19083, Jira:RHELDOCS-19269, Jira:RHELDOCS-18080, Jira:RHELDOCS-18544, Jira:RHELDOCS-18674, Jira:RHELDOCS-18672, Jira:RHELDOCS-19015, Jira:RHELDOCS-19172, Jira:RHELDOCS-19016, Jira:RHELDOCS-18991
anaconda	Jira:RHEL-38407, Jira:RHEL-33892, Jira:RHEL-58834
annobin	Jira:RHEL-526
ansible-freeipa	Jira:RHEL-35566
bind-dyndb-ldap	Jira:RHEL-30556
binutils	Jira:RHEL-36305
bootc-image-builder-container	Jira:RHEL-34807
ca-certificates	Jira:RHEL-50293
certmonger	Jira:RHEL-40922
clevis	Jira:RHEL-29279

Component	Tickets
cloud-init	Jira:RHEL-29720, Jira:RHEL-65849
cockpit	Jira:RHEL-4032
cockpit-machines	Jira:RHEL-31993
container-tools	Jira:RHEL-33571, Jira:RHEL-33573, Jira:RHEL-32715
crypto-policies	Jira:RHEL-50655, Jira:RHEL-50464, Jira:RHEL-50106
cryptsetup	Jira:RHEL-33395
dnf	Jira:RHEL-12355, Jira:RHEL-38831, Jira:RHEL-40382
dnf-plugins-core	Jira:RHEL-23706
dnsconfd	Jira:RHEL-34791
dyninst	Jira:RHEL-49597
elfutils	Jira:RHEL-29197
flatpak-runtime-container	Jira:RHEL-24332
gcc	Jira:RHEL-45041, Jira:RHEL-33254, Jira:RHEL-24760
gdb	Jira:RHEL-33256
glibc	Jira:RHEL-25045, Jira:RHEL-25850, Jira:RHEL-25530
gnome-online-accounts	Jira:RHEL-40831
gnutls	Jira:RHEL-42514, Jira:RHEL-50011, Jira:RHEL-59212, Jira:RHEL-58640
golang	Jira:RHEL-46971
grafana	Jira:RHEL-35761
grafana-pcp	Jira:RHEL-45646
ipa	Jira:RHEL-4879, Jira:RHEL-46607, Jira:RHEL-33818, Jira:RHEL-12154, Jira:RHEL-59265
jose	Jira:RHEL-38084

Component	Tickets
kdump-utils	Jira:RHEL-63071, Jira:RHEL-50736
kea	Jira:RHEL-9306
kernel	Bugzilla:2013650, Bugzilla:2000616
kernel / **Debugging-Tracing** / **kexec - kdump**	Jira:RHEL-29272
kernel / **Security**	Jira:RHEL-26170
kernel / **Virtualization** / **ESXi**	Jira:RHEL-41133
keylime	Jira:RHEL-51279
keylime-agent-rust	Jira:RHEL-38409
ksh	Jira:RHEL-45981
libabigail	Jira:RHEL-30014
libcap	Jira:RHEL-31988, Jira:RHEL-33498
libkcapi	Jira:RHEL-50457
librepo	Jira:RHEL-47106
libreswan	Jira:RHEL-52935, Jira:RHEL-51880
libslirp	Jira:RHEL-45147
libssh	Jira:RHEL-30437
llvm-toolset	Jira:RHEL-28056
lsscsi	Jira:RHEL-32144
mysql	Jira:RHEL-36050
nbdkit	Jira:RHEL-32748
net-snmp	Jira:RHEL-44478
nginx	Jira:RHEL-33742

Component	Tickets
nodejs	Jira:RHEL-35992
nss	Jira:RHEL-46839, Jira:RHEL-39732, Jira:RHEL-36299, Jira:RHEL-44995
opencryptoki	Jira:RHEL-24038
openssh	Jira:RHEL-42635, Jira:RHEL-37324, Jira:RHEL-45002
openssl	Jira:RHEL-54156, Jira:RHEL-40408, Jira:RHEL-36659, Jira:RHEL-39962, Jira:RHEL-45704
p11-kit	Jira:RHEL-46898
pacemaker	Jira:RHEL-38543
pcs	Jira:RHEL-35670, Jira:RHEL-36612, Jira:RHEL-38491, Jira:RHEL-38489, Jira:RHEL-38487, Jira:RHEL-23048, Jira:RHEL-38493, Jira:RHEL-38484, Jira:RHEL-38486, Jira:RHEL-38478, Jira:RHEL-38479, Jira:RHEL-34792, Jira:RHEL-29739, Jira:RHEL-34783
pkcs11-provider	Jira:RHEL-29672, Jira:RHEL-40124
podman	Jira:RHEL-34604, Jira:RHEL-33566, Jira:RHEL-34611, Jira:RHEL-34613, Jira:RHEL-34606, Jira:RHEL-40639, Jira:RHEL-40643, Jira:RHEL-52238, Jira:RHEL-52240, Jira:RHEL-52247, Jira:RHEL-32266, Jira:RHEL-40641
policycoreutils	Jira:RHEL-40233
polkit	Jira:RHEL-55287
postgresql	Jira:RHEL-35993
pykickstart	Jira:RHEL-34829
python-blivet	Jira:RHEL-45175
qemu-kvm	Jira:RHEL-58928
rear	Jira:RHEL-46613
rhel-bootc-container	Jira:RHEL-34859

Component	Tickets
rhel-system-roles	Jira:RHEL-34893, Jira:RHEL-37551, Jira:RHEL-40798, Jira:RHEL-34879, Jira:RHEL-34884, Jira:RHEL-34890, Jira:RHEL-34891, Jira:RHEL-34892, Jira:RHEL-40181, Jira:RHEL-40797, Jira:RHEL-45718, Jira:RHEL-46855, Jira:RHEL-48230, Jira:RHEL-48609, Jira:RHEL-50288, Jira:RHEL-50289, Jira:RHEL-50291, Jira:RHEL-53901, Jira:RHEL-34828, Jira:RHEL-34887, Jira:RHEL-34886, Jira:RHEL-34881, Jira:RHEL-34888, Jira:RHEL-34889, Jira:RHEL-34895, Jira:RHEL-34907, Jira:RHEL-38456, Jira:RHEL-40759, Jira:RHEL-40760, Jira:RHEL-40795, Jira:RHEL-50104, Jira:RHEL-57100, Jira:RHEL-45944
rust	Jira:RHEL-30071
selinux-policy	Jira:RHEL-36094, Jira:RHEL-33844, Jira:RHEL-46893
setools	Jira:RHEL-29967
sg3_utils	Jira:RHEL-412
slapi-nis	Jira:RHEL-34186
sos	Jira:RHEL-35945, Jira:RHEL-22389, Jira:RHEL-24523, Jira:RHEL-30893
sssd	Jira:RHEL-50243
stunnel	Jira:RHEL-33749
systemtap	Jira:RHEL-29529
tbb	Jira:RHEL-33633
valgrind	Jira:RHEL-29535
virt-v2v	Jira:RHEL-37687, Jira:RHEL-36712
zlib	Jira:RHEL-24058

Component	Tickets
other	Jira:RHELDOCS-18402, Jira:RHELDOCS-18869, Jira:RHELDOCS-18761, Jira:RHELDOCS-18997, Jira:RHELDOCS-18197, Jira:RHELDOCS-19185, Jira:RHELDOCS-19191, Jira:RHELDOCS-19197, Jira:RHELDOCS-19263, Jira:RHEL-59102, Jira:RHELDOCS-18585, Jira:RHELDOCS-18398, Jira:RHELDOCS-18522, Jira:RHELDOCS-18769, Jira:RHELDOCS-19162, Jira:RHELDOCS-18532, Jira:RHELDOCS-18880, Jira:RHELDOCS-18902, Jira:RHELDOCS-18425, Jira:RHELDOCS-16362, Jira:RHELDOCS-18925, Jira:RHELDOCS-18776, Jira:RHELDOCS-18819, Jira:RHELDOCS-19059, Jira:RHELDOCS-18472, Jira:RHELDOCS-18201, Jira:RHELDOCS-18770, Jira:RHELDOCS-16800, Jira:RHELDOCS-17465, Jira:RHELDOCS-18408, Jira:RHELDOCS-19009, Jira:RHELDOCS-19010, Jira:RHELDOCS-19071, Jira:RHELDOCS-19066, Jira:RHELDOCS-18388, Jira:RHELDOCS-18389, Jira:RHELDOCS-18390, Jira:RHELDOCS-17682, Jira:RHELDOCS-19221, Jira:RHELDOCS-19222, Jira:RHELDOCS-19005, Jira:RHELDOCS-19094, Jira:RHELDOCS-19267, Jira:RHELDOCS-18839, Jira:RHELDOCS-18818, Jira:RHELDOCS-18736, Jira:RHELDOCS-18492, Jira:RHELDOCS-18485, Jira:RHELDOCS-18426, Jira:RHELDOCS-18423, Jira:RHELDOCS-18417, Jira:RHELDOCS-18416, Jira:RHELDOCS-18415, Jira:RHELDOCS-18414, Jira:RHELDOCS-18413, Jira:RHELDOCS-18412, Jira:RHELDOCS-18411, Jira:RHELDOCS-18410, Jira:RHELDOCS-19051, Jira:RHELDOCS-18989, Jira:RHELDOCS-18700, Jira:RHELDOCS-18903, Jira:RHELDOCS-18904, Jira:RHELDOCS-18491, Jira:RHELDOCS-18672, Jira:RHELDOCS-18815, Jira:RHELDOCS-19015, Jira:RHELDOCS-19172, Jira:RHELDOCS-18471, Jira:RHELDOCS-18991

APPENDIX B. REVISION HISTORY

0.0-3

Wed February 19 2025, Gabriela Fialová (gfialova@redhat.com)

- Added a New Feature in Jira:RHELDOCS-18391 (Infrastructure services)

0.0-2

Thu January 16 2025, Gabriela Fialová (gfialova@redhat.com)

- Added a Rebase in Jira:RHEL-54839 (Security)

- Added a Rebase in Jira:RHEL-53981 (Security)

- Added a Known Issue in Jira:RHEL-56981 (Virtualization)

0.0-1

Fri December 13 2024, Brian Angelica (bangelic@redhat.com)

- Updated a New Feature in Jira:RHELDOCS-18902 (Installer and image creation)

0.0-0

Wed November 13 2024, Gabriela Fialová (gfialova@redhat.com)

- Release of the Red Hat Enterprise Linux 10.0 Beta Release Notes.