Red Hat Enterprise Linux 8.5 Beta

8.5 Release Notes

Release Notes for Red Hat Enterprise Linux 8.5 Beta

Last Updated: 2021-11-02

Red Hat Enterprise Linux 8.5 Beta 8.5 Release Notes

Release Notes for Red Hat Enterprise Linux 8.5 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 8.5 Beta and document known problems in this release, as well as notable bug fixes, Technology Previews, deprecated functionality, and other details.

Table of Contents

THIS IS A BETA VERSION!

This document is provided as a preview and only includes or highlights features that are new as part of the public Beta. It is under development and is subject to substantial change. Consider the included information incomplete and use it with caution. This content will later be incorporated into the regular product documentation available at Product Documentation for Red Hat Enterprise Linux 8 .

MAKING OPEN SOURCE MORE INCLUSIVE

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

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

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

- For simple comments on specific passages, make sure you are viewing the documentation in the Multi-page HTML format. Highlight the part of text that you want to comment on. Then, click the **Add Feedback** pop-up that appears below the highlighted text, and follow the displayed instructions.
- For submitting more complex feedback, create a Bugzilla ticket:
    1. Go to the Bugzilla website.
    2. As the Component, use **Documentation**.
    3. Fill in the **Description** field with your suggestion for improvement. Include a link to the relevant part(s) of documentation.
    4. Click **Submit Bug**.

CHAPTER 1. OVERVIEW

1.1. MAJOR CHANGES IN RHEL 8.5

Security

The system-wide **cryptographic policies** support scopes and wildcards for directives in custom policies. You can now enable different sets of algorithms for different back ends.

The **Rsyslog** log processing application has been updated to version 8.2102.0-5. This update introduces, among other improvements, the OpenSSL network stream driver. This implements **TLS-protected transport** using the OpenSSL library into Rsyslog.

The **SCAP Security Guide** project now provides several new profiles and improvements of existing profiles:

- A new profile aligned with the Australian Cyber Security Centre Information Security Manual (ACSC ISM).
- The Center for Internet Security (CIS) profile restructured into four different profiles (Workstation Level 1, Workstation Level 2, Server Level 1, Server Level 2).
- The Security Technical Implementation Guide (STIG) security profile updated to version V1R3.
- A new STIG profile compatible with **Server with GUI** installations.
- A new French National Security Agency (ANSSI) High Level profile, which completes the availability of profiles for all ANSSI-BP-028 v1.2 hardening levels in the **SCAP Security Guide**.

With these enhancements, you can install a system that conforms with one of these security baselines and use the **OpenSCAP** suite for checking security compliance and remediation using the risk-based approach for security controls defined by the relevant authorities.

See New features - Security for more information.

The new **RHEL VPN System Role** makes it easier to set up secure and properly configured IPsec tunneling and virtual private networking (VPN) solutions on across large numbers of hosts. For more information, see New Features - Red Hat Enterprise Linux System Roles and the Configuring VPN connections with IPsec by using the RHEL VPN System Role chapter in RHEL 8.5 Beta product documentation.

Networking

NetworkManager now supports configuring a device to accept all traffic. You can configure this feature, for example using the **nmcli** utility.

The **firewalld** service supports forwarding traffic between different interfaces or sources within a zone.

The **firewalld** service supports filtering traffic that is forwarded between zones.

Dynamic programming languages, web and database servers

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

- **Ruby 3.0**
- **nginx 1.20**
- **Node.js 16**

The following components have been upgraded:

- **PHP** to version 7.4.19
- **Squid** to version 4.15
- **Mutt** to version 2.0.7

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

Compilers and development tools

The following compiler toolsets have been updated:

- **GCC Toolset 11**
- **LLVM Toolset 12.0.1**
- **Rust Toolset 1.54.0**
- **Go Toolset 1.16.7**

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

Red Hat Enterprise Linux System Roles

High Availability Cluster RHEL System Role is available as a Technology Preview for the 8.5 Beta Release.

See Section 4.16, "Red Hat Enterprise Linux System Roles" 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
- Product Life Cycle Checker
- Kickstart Generator
- Kickstart Converter
- Red Hat Enterprise Linux Upgrade Helper
- Red Hat Satellite Upgrade Helper
- Red Hat Code Browser
- JVM Options Configuration Tool
- Red Hat CVE Checker
- Red Hat Product Certificates

- Load Balancer Configuration Tool
- Yum Repository Configuration Helper
- Red Hat Memory Analyzer
- Kernel Oops Analyzer
- Red Hat Product Errata Advisory Checker

1.3. ADDITIONAL RESOURCES

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

CHAPTER 2. ARCHITECTURES

Red Hat Enterprise Linux 8.5 Beta is distributed with the kernel version 4.18.0-326, which provides support for the following architectures:

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

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

CHAPTER 3. DISTRIBUTION OF CONTENT IN RHEL 8

3.1. INSTALLATION

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

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

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

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

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

3.2. REPOSITORIES

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

- BaseOS
- AppStream

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

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

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

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

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

3.3. APPLICATION STREAMS

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

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

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

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

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

3.4. PACKAGE MANAGEMENT WITH YUM/DNF

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

For more details, see the following documentation:

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

CHAPTER 4. NEW FEATURES

This part describes new features and major enhancements introduced in Red Hat Enterprise Linux 8.5 Beta.

4.1. INSTALLER AND IMAGE CREATION

Image Builder now supports filesystem configuration

With this enhancement, you can specify custom filesystem configuration in your blueprints and you can create images with the desired disk layout. As a result, by having non-default layouts, you can benefit from security benchmarks, consistency with existing setups, performance, and protection against out-of-disk errors.

To customize the filesystem configuration in your blueprint, set the following customization:

```
[[customizations.filesystem]]
mountpoint = "MOUNTPOINT"
size = MINIMUM-PARTITION-SIZE
```

(BZ#2011448)

RHEL for Edge now supports a Simplified Installer

This enhancement enables Image Builder to build the RHEL for Edge Simplified Installer (**edge-simplified-installer**) and RHEL for Edge Raw Images (**edge-raw-image**).

RHEL for Edge Simplified Installer enables you to specify a new blueprint option, **installation_device** and thus, perform an unattended installation to a device. To create the raw image, you must provide an existing OSTree commit. It results in a raw image with the existing commit deployed in it. The installer will use this raw image to the specified installation device.

Additionally, you can also use Image Builder to build RHEL for Edge Raw Images. These are compressed raw images that contain a partition layout with an existing deployed OSTree commit in it. You can install the RHEL for Edge Raw Images to flash on a hard drive or booted in a virtual machine.

(BZ#1937854)

Ability to override official repositories available

By default, the **osbuild-composer** backend has its own set of official repositories defined in the **/usr/share/osbuild-composer/repositories** directory. Consequently, it does not inherit the system repositories located in the **/etc/yum.repos.d/** directory. You can now override the official repositories. To do that, define overrides in the **/etc/osbuild-composer/repositories** and, as a result, the files located there take precedence over those in the **/usr** directory.

(BZ#1915351)

Warnings for deprecated kernel boot arguments

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

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

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

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

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

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

(BZ#1897657)

4.2. RHEL FOR EDGE

Greenboot services now enabled by default

Previously, the greenboot services were not present in the default presets so, when the greenboot package was installed, users had to manually enable these greenboot services. With this update, the greenboot services are now present in the default presets configuration and users are no longer required to manually enable it.

(BZ#1935177)

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

When creating OSTree commits for **RHEL for Edge** images, only one kernel package can be installed at a time, otherwise the commit creation fails in **rpm-ostree**. This prevents RHEL for Edge from adding alternative kernels, in particular, the real-time kernel (**kernel-rt**). With this enhancement, when creating a blueprint for RHEL for Edge image using the CLI, you can define the name of the kernel to be used in an image, by setting the **customizations.kernel.name** key. If you do not specify any kernel name, the image include the default kernel package.

(BZ#1960043)

4.3. SOFTWARE MANAGEMENT

RPM now has read-only support for the sqlite database backend

The ability to query an RPM database based on **sqlite** may be desired when inspecting other root directories, such as containers.This update adds read-only support for the RPM **sqlite** database backend. As a result, it is now possible to query packages installed in a UBI 9 or Fedora container from the host RHEL 8. To do that with Podman:

1. Mount the container’s file system with the **podman mount** command.
2. Run the **rpm -qa** command with the **--root** option pointing to the mounted location.

Note that RPM on RHEL 8 still uses the BerkeleyDB database (**bdb**) backend.

(BZ#1938928)

libmodulemd rebased to version 2.12.1

The **libmodulemd** packages have been rebased to version 2.12.1. Notable changes include:

- Added support for version 1 of the **modulemd-obsoletes** document type, which provides information about a stream obsoleting another one, or a stream reaching its end of life.
- Added support for version 3 of the **modulemd-packager** document type, which provides a packager description of a module stream content for a module build system.
- Added support for the **static_context** attribute of the version 2 **modulemd** document type. With that, a module context is now defined by a packager instead of being generated by a module build system.
- Now, a module stream value is always serialized as a quoted string.

(BZ#1894573)

libmodulemd rebased to version 2.13.0

The **libmodulemd** packages have been rebased to version 2.13.0, which provides the following notable changes over the previous version:

- Added support for delisting demodularized packages from a module.
- Added support for validating **modulemd-packager-v3** documents with a new **--type** option of the **modulemd-validator** tool.
- Fortified parsing integers.
- Fixed various **modulemd-validator** issues.

(BZ#1984402)

sslverifystatus has been added to dnf configuration

With this update, when **sslverifystatus** option is enabled, **dnf** checks each server certificate revocation status using the **Certificate Status Request** TLS extension (OCSP stapling). As a result, when a revoked certificate is encountered, **dnf** refuses to download from its server.

(BZ#1814383)

4.4. SHELLS AND COMMAND-LINE TOOLS

Relax-and-Recover (ReaR) has been updated to version 2.6

ReaR has been updated to version 2.6. Notable bug fixes and enhancements include:

- Added support for **eMMC** devices.
- By default, all kernel modules are included in the rescue system. To include specific modules, set the **MODULES** array variable in the configuration file as: **MODULES=(mod1 mod2)**
- On **x86_64** and **ppc64le**, a new configuration variable **GRUB2_INSTALL_DEVICES** is introduced to control the location of the bootloader installation. See the description in **/usr/share/rear/conf/default.conf** for more details.
- Improved backup of multipath devices.
- Files under /**media**, /**run**, /**mnt**, /**tmp** are automatically excluded from backups as these directories are known to contain removable media or temporary files. See the description of the AUTOEXCLUDE_PATH variable in /**usr/share/rear/conf/default.conf**.

- **CLONE_ALL_USERS_GROUPS=true** is now the default. See the description in **/usr/share/rear/conf/default.conf** for more details.

(BZ#1988493)

The **modulemd-tools** package is now available

With this update, the **modulemd-tools** package has been introduced which provides tools for parsing and generating **modulemd** YAML files.

To install **modulemd-tools**, use:

```
# yum install modulemd-tools
```

(BZ#1924850)

opencryptoki rebased to version 3.16.0

opencryptoki has been upgraded to version 3.16.0. Notable bug fixes and enhancements include:

- Improved the **protected-key** option and support for the **attribute-bound keys** in the **EP11** core processor.

- Improved the import and export of secure key objects in the **cycle-count-accurate** (CCA) processor.

(BZ#1919223)

lsvpd rebased to version 1.7.12

lsvpd has been upgraded to version 1.7.12. Notable bug fixes and enhancements include:

- Added the UUID property in **sysvpd**.

- Improved the **NVMe** firmware version.

- Fixed PCI device manufacturer parsing logic.

- Added **recommends clause** to the **lsvpd** configuration file.

(BZ#1844428)

ppc64-diag rebased to version 2.7.7

ppc64-diag has been upgraded to version 2.7.7. Notable bug fixes and enhancements include:

- Improved unit test cases.

- Added the UUID property in **sysvpd**.

- The **rtas_errd** service does not run in the Linux containers.

- The obsolete logging options are no longer available in the **systemd** service files.

(BZ#1779206)

IPMI modules available in the **rhel_mgmt** Collection

This update provides support to the **IPMI** modules. The Intelligent Platform Management Interface (IPMI) is a specification for a set of management interfaces to communicate with baseboard management controller (BMC) devices. The **IPMI** modules are available in the **rhel_mgmt** Collection and you can install it by using the **ansible-collection-redhat-rhel_mgmt** package.

(BZ#1843859)

udftools 2.3 is now added to RHEL 8.5

udftools are userspace utilities for manipulating Universal Disk Format (UDF) file systems. With this enhancement, **udftools** provides the following set of tools:

- **cdrwtool** - It performs actions like blank, format, quick setup, and write to the DVD-R/CD-R/CD-RW media.
- **mkfs.udf**, **mkudffs** - It creates a Universal Disk Format (UDF) filesystem.
- **pktsetup** - It sets up and tears down the packet device.
- **udfinfo** - It shows information about the Universal Disk Format (UDF) file system.
- **udflabel** - It shows or changes the Universal Disk Format (UDF) file system label.
- **wrudf** - It provides an interactive shell with **cp**, **rm**, **mkdir**, **rmdir**, **ls**, and **cd** operations on the existing Universal Disk Format (UDF) file system.

(BZ#1882531)

Tesseract 4.1.1 is now present in RHEL 8.5

Tesseract is an open-source OCR (optical character reading) engine and has the following features:

- Starting with **tesseract** version 4, character recognition is based on Long Short-Term Memory (LSTM) neural networks.
- Supports UTF-8.
- Supports plain text, hOCR (HTML), PDF, and TSV output formats.

(BZ#1826085)

Errors when restoring LVM with thin pools do not happen anymore

With this enhancement, ReaR now detects when thin pools and other logical volume types with kernel metadata (for example, RAIDs and caches) are used in a volume group (VG) and switches to a mode where it recreates all the logical volumes (LVs) in the VG using lvcreate commands. Therefore, LVM with thin pools are restored without any errors.

NOTE

This new method does not preserve all the LV properties, for example LVM UUIDs. A restore from the backup should be tested before using ReaR in a Production environment in order to determine whether the recreated storage layout matches the requirements.

(BZ#1747468)

Net-SNMP now detects RSA and ECC certificates

Previously, Net-Simple Network Management Protocol (Net-SNMP) detected only Rivest, Shamir, Adleman (RSA) certificates. This enhancement adds support for Elliptic Curve Cryptography (ECC). As a result, Net-SNMP now detects RSA and ECC certificates.

(BZ#1919714)

FCoE option is changed to rd.fcoe

Previously, the man page for **dracut.cmdline** documented **rd.nofcoe=0** as the command to turn off Fibre Channel over Ethernet (FCoE).

With this update, the command is changed to **rd.fcoe**. To disable FCoE, run the command **rd.fcoe=0**.

For further information on FCoE see, Configuring Fibre Channel over Ethernet

(BZ#1929201)

4.5. INFRASTRUCTURE SERVICES

linuxptp rebased to version 3.1

linuxptp package has been updated to version 3.1. Notable bug fixes and enhancements include:

- Added **ts2phc** program for synchronization of Precision Time Protocol (PTP) hardware clock to Pulse Per Second (PPS) signal.
- Added support for the automotive profile.
- Added support for client event monitoring.

(BZ#1895005)

chrony rebased to version 4.1

chrony has been updated to version 4.1. Notable bug fixes and enhancements include:

- Added support for Network Time Security (NTS) authentication.
- By default, the Authenticated Network Time Protocol (NTP) sources are trusted over non-authenticated NTP sources. Add the **autselectmode ignore** argument in the **chrony.conf** file to restore the original behavior.
- The support for authentication with **RIPEMD** keys - **RMD128**, **RMD160**, **RMD256**, **RMD320** is no longer available.
- The support for long non-standard MACs in NTPv4 packets is no longer available. If you are using **chrony 2.x**, **non-MD5/SHA1** keys, you need to configure **chrony** with the **version 3** option.

(BZ#1895003)

PowerTop rebased to version 2.14

PowerTop has been upgraded to version 2.14. This is an update adding Alder Lake, Sapphire Rapids, and Rocket Lake platforms support.

(BZ#1834722)

TuneD now moves unnecessary IRQs to housekeeping CPUs

Network device drivers like **i40e**, **iavf**, **mlx5**, evaluate the online CPUs to determine the number of queues and hence the **MSIX** vectors to be created.

In low-latency environments with a large number of isolated and very few housekeeping CPUs, when TuneD tries to move these device IRQs to the housekeeping CPUs it fails due to the per CPU vector limit.

With this enhancement, TuneD explicitly adjusts the numbers of network device channels (and hence MSIX vectors) as per the housekeeping CPUs. Therefore, all the device IRQs can now be moved on the housekeeping CPUs to achieve low latency.

(BZ#1951992)

4.6. SECURITY

socat rebased to 1.7.4

The **socat** packages have been upgraded from version 1.7.3 to 1.7.4, which provides many bug fixes and improvements. Most notably:

- **GOPEN** and **UNIX-CLIENT** addresses now support **SEQPACKET** sockets.
- The generic **setsockopt-int** and related options are, in the case of listening or accepting addresses, applied to the connected sockets. To enable setting options on a listening socket, the **setsockopt-listen** option is now available.
- Added the **-r** and **-R** options for a raw dump of transferred data to a file.
- Added the **ip-transparent** option and the **IP_TRANSPARENT** socket option.
- **OPENSSL-CONNECT** now automatically uses the SNI feature and the **openssl-no-sni** option turns SNI off. The **openssl-snihost** option overrides the value of the **openssl-commonname** option or the server name.
- Added the **accept-timeout** and **listen-timeout** options.
- Added the **ip-add-source-membership** option.
- **UDP-DATAGRAM** address now does not check peer port of replies as it did in 1.7.3. Use the **sourceport** optioon if your scenario requires the previous behavior.
- New **proxy-authorization-file** option reads **PROXY-CONNECT** credentials from a file and enables to hide this data from the process table.
- Added **AF_VSOCK** support for **VSOCK-CONNECT** and **VSOCK-LISTEN** addresses.

(BZ#1947338)

crypto-policies rebased to 20210617

The **crypto-policies** packages have been upgraded to upstream version 20210617, which provides a number of enhancements and bug fixes over the previous version, most notably:

- You can now use scoped policies to enable different sets of algorithms for different back ends. Each configuration directive can now be limited to specific protocols, libraries or services.

Please refer to the **crypto-policies(7)** man page for the complete list of available scopes and details on the new syntax. For example, the following directive allows using AES-256-CBC cipher with the SSH protocol, impacting both the **libssh** library and the OpenSSH suite:

```
cipher@SSH = AES-256-CBC+
```

- Directives can now use asterisks for specifying multiple values using wildcards. For example, the following directive disables all CBC mode ciphers for applications using **libssh**:

  ```
  cipher@libssh = -*-CBC
  ```

  Note that future updates can introduce new algorithms matched by the current wildcards.

(BZ#1960266)

crypto-policies now support AES-192 ciphers in custom policies

The system-wide cryptographic policies now support the following values for the **cipher** option in custom policies and subpolicies: **AES-192-GCM**, **AES-192-CCM**, **AES-192-CTR**, and **AES-192-CBC**. As a result, you can enable the **AES-192-GCM** and **AES-192-CBC** ciphers for the Libreswan application and the **AES-192-CTR** and **AES-192-CBC** ciphers for the **libssh** library and the OpenSSH suite through **crypto-policies**.

(BZ#1876846)

Feature: ciphers using CBC mode will be disabled when using FUTURE crypto-policy

Reason: to keep FUTURE security policy up with the changing

Result: components respecting crypto-policies will have CBC mode disabled when FUTURE policy is active

(BZ#1933016)

Adding new kernel AVC tracepoint

With this enhancement, a new **avc:selinux_audited** kernel tracepoint is added that triggers when an SELinux denial is to be audited. This feature allows for more convenient low-level debugging of SELinux denials. The new tracepoint is available for tools such as **perf**.

(BZ#1954024)

New ACSC ISM profile in the SCAP Security Guide

The **scap-security-guide** packages now provide the Australian Cyber Security Centre (ACSC) Information Security Manual (ISM) compliance profile and a corresponding Kickstart file. With this enhancement, you can install a system that conforms with this security baseline and use the OpenSCAP suite for checking security compliance and remediation using the risk-based approach for security controls defined by ACSC.

(BZ#1955373)

SCAP Security Guide rebased to 0.1.57

The **scap-security-guide** packages have been rebased to upstream version 0.1.57, which provides several bug fixes and improvements. Most notably:

- The Australian Cyber Security Centre (**ACSC**) Information Security Manual (**ISM**) profile has been introduced. The profile extends the Essential Eight profile and adds more security controls defined in the ISM.
- The Center for Internet Security (**CIS**) profile has been restructured into four different profiles respecting levels of hardening and system type (server and workstation) as defined in the official CIS benchmarks.
- The Security Technical Implementation Guide (**STIG**) security profile has been updated, and implements rules from the recently-released version V1R3.
- The Security Technical Implementation Guide with GUI (**STIG with GUI**) security profile has been introduced. The profile derives from the STIG profile and is compatible with RHEL installations that select the **Server with GUI** package selection.
- The **ANSSI** High level profile, which is based on the ANSSI BP-028 recommendations from the French National Security Agency (ANSSI), has been introduced. This contains a profile implementing rules of High hardening levels.

(BZ#1966577)

OpenSCAP rebased to 1.3.5

The OpenSCAP packages have been rebased to upstream version 1.3.5. Notable fixes and enhancements include:

- Enabled Schematron-based validation by default for the **validate** command of **oval** and **xccdf** modules.
- Added SCAP 1.3 source data stream Schematron.
- Added XML signature validation.
- Allowed clamping **mtime** to **SOURCE_DATE_EPOCH**.
- Added **severity** and **role** attributes.
- Support for **requires** and **conflicts** elements of the Rule and Group (XCCDF).
- Kubernetes remediation in the HTML report.
- Handling 'gpfs', 'proc' and 'sysfs' file systems as non-local.
- Fixed handling of common options styled like`--arg=val`.
- Fixed behavior of the **StateType** operator.
- Namespace ignored in XPath expressions (**xmlfilecontent**) to allow for incomplete XPath queries.
- Fixed a problem that led to a warning about the presence of obtrusive data.
- Fixed multiple segfaults and a broken test in the **--stig-viewer** feature.
- Fixed the **TestResult/benchmark/@href** attribute.
- Fixed many memory management issues.

- Fixed many memory leaks.

(BZ#1953092)

Validation of digitally signed SCAP source data streams

To conform with the Security Content Automation Protocol (SCAP) 1.3 specifications, OpenSCAP now validates digital signatures of digitally signed SCAP source data streams. As a result, OpenSCAP validates the digital signature when evaluating a digitally signed SCAP source data stream. The signature validation is performed automatically while loading the file. Data streams with invalid signatures are rejected, and OpenSCAP does not evaluate their content. OpenSCAP uses the XML Security Library with the OpenSSL cryptography library to validate the digital signature.

You can skip the signature validation by adding the **--skip-signature-validation** option to the **oscap xccdf eval** command.

CAUTION

OpenSCAP does not address the trustworthiness of certificates or public keys that are part of the **KeyInfo** signature element and that are used to verify the signature. You should verify such keys by yourselves to prevent evaluation of data streams that have been modified and signed by bad actors.

(BZ#1966612)

New DISA STIG profile compatible with Server with GUI installations

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

(BZ#1970137)

STIG security profile updated to version V1R3

With the RHBA-2021:77315-01 advisory, the **DISA STIG for Red Hat Enterprise Linux 8** profile in the SCAP Security Guide has been updated to align with the latest version **V1R3**. The profile is now also more stable and better aligns with the RHEL 8 STIG (Security Technical Implementation Guide) manual benchmark provided by the Defense Information Systems Agency (DISA).

This second iteration brings approximately 90% of coverage with regards to the STIG. You should use only the current version of this profile because older versions are no longer valid.

WARNING

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

(BZ#1993056)

Three new CIS profiles in SCAP Security Guide

Three new compliance profiles aligned with the Center for Internet Security (CIS) Red Hat Enterprise Linux 8 Benchmark have been introduced to the SCAP Security Guide. The CIS RHEL 8 Benchmark provides different configuration recommendations for "Server" and "Workstation" deployments, and defines two levels of configuration, "level 1" and "level 2" for each deployment. The CIS profile previously shipped in RHEL8 represented only the "Server Level 2". The three new profiles complete the scope of the CIS RHEL8 Benchmark profiles, and you can now more easily evaluate your system against CIS recommendations.

All currently available CIS RHEL 8 profiles are:

Workstation Level 1	**xccdf_org.ssgproject.content_profile_cis_workstation_l1**
Workstation Level 2	**xccdf_org.ssgproject.content_profile_cis_workstation_l2**
Server Level 1	**xccdf_org.ssgproject.content_profile_cis_server_l1**
Server Level 2	**xccdf_org.ssgproject.content_profile_cis**

(BZ#1993197)

Performance of remediations for Audit improved by grouping similar system calls

Previously, Audit remediations generated an individual rule for each system call audited by the profile. This led to large numbers of audit rules, which degraded performance. With this enhancement, remediations for Audit can group rules for similar system calls with identical fields together into a single rule, which improves performance.

Examples of system calls grouped together:

> -a always, exit -F arch=b32 -S chown, fchown, fchownat, lchown -F auid>=1000 -F auid!=unset -F key=perm_mod

> -a always, exit -F arch=b32 -S unlink, unlinkat, rename, renameat, rmdir -F auid>=1000 -F auid!=unset -F key=delete

> -a always, exit -F arch=b32 -S chown, fchown, fchownat, lchown -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=unsuccesful-perm-change

> -a always, exit -F arch=b32 -S unlink, unlinkat, rename, renameat -F auid>=1000 -F auid!=unset -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=unsuccessful-delete

(BZ#1876483)

Added profile for ANSSI-BP-028 High level

The ANSSI High level profile, based on the ANSSI BP-028 recommendations from the French National Security Agency (ANSSI), has been introduced. This completes the availability of profiles for all ANSSI-

BP-028 v1.2 hardening levels in the **SCAP Security Guide**. With the new profile, you can harden the system to the recommendations from ANSSI for GNU/Linux Systems at the High hardening level. As a result, you can configure and automate compliance of your RHEL 8 systems to the strictest hardening level by using the ANSSI Ansible Playbooks and the ANSSI SCAP profiles.

(BZ#1955183)

OpenSSL added for encrypting Rsyslog TCP and RELP traffic

The OpenSSL network stream driver has been added to Rsyslog. This driver implements TLS-protected transport using the OpenSSL library. This provides additional functionality compared to the stream driver using the GnuTLS library. As a result, you can now use either OpenSSL or GnuTLS as an Rsyslog network stream driver.

(BZ#1891458)

Rsyslog rebased to 8.2102.0-5

The **rsyslog** packages have been rebased to upstream version 8.2102.0-5, which provides the following notable changes over the previous version:

- Added the **exists()** script function to check whether a variable exists or not, for example **$!path!var**.
- Added support for setting OpenSSL configuration commands with a new configuration parameter **tls.tlscfgcmd** for the **omrelp** and **imrelp** modules.
- Added new rate-limit options to the **omfwd** module for rate-limiting syslog messages sent to the remote server:
  - **ratelimit.interval** specifies the rate-limiting interval in seconds.
  - **ratelimit.burst** specifies the rate-limiting burst in the number of messages.
- Rewritten the **immark** module with various improvements.
- Added the **max sessions** config parameter to the **imptcp** module. The maximum is measured per instance, not globally across all instances.
- Added the **rsyslog-openssl** subpackage; this network stream driver implements TLS-protected transport using the OpenSSL library.
- Added per-minute rate limiting to the **imfile** module with the **MaxBytesPerMinute** and **MaxLinesPerMinute** options. These options accept integer values and limit the number of bytes or lines that may be sent in a minute.
- Added support to the **imtcp** and **omfwd** module to configure a maximum depth for the certificate chain verification with the **streamdriver.TlsVerifyDepth** option.

(BZ#1932795)

4.7. NETWORKING

Support for pause parameter of ethtool in NetworkManager

Non auto-pause parameters need to be set explicitly on a specific network interface in certain cases. Previously, NetworkManager could not pause the control flow parameters of **ethtool** in **nmstate**. To disable the auto negotiation of the pause parameter and enable RX/TX pause support explicitly, use the following command:

```
# nmcli connection modify enp1s0 ethtool.pause-autoneg no ethtool.pause-rx true ethtool.pause-tx true
```

(BZ#1899372)

New property in NetworkManager for setting physical and virtual interfaces in promiscuous mode

With this update the **802-3-ethernet.accept-all-mac-addresses** property has been added to NetworkManager for setting physical and virtual interfaces in the **accept all MAC addresses** mode. With this, the kernel can accept network packages targeting current interfaces' MAC address in the **accept all MAC addresses** mode. To enable **accept all MAC addresses** mode on eth1, use the following command:

```
$ sudo nmcli c add type ethernet  ifname eth1 connection.id eth1  802-3-ethernet.accept-all-mac-addresses true
```

(BZ#1942331)

NetworkManager rebased to version 1.32.10

The **NetworkManager** packages have been upgraded to upstream version 1.32.10, which provides a number of enhancements and bug fixes over the previous version.

For further information about notable changes, read the upstream release notes for this version.

(BZ#1934465)

NetworkManager now supports **nftables** as firewall back end

This enhancement adds support for the **nftables** firewall framework to NetworkManager. To switch the default back end from **iptables** to **nftables**:

1. Create the **/etc/NetworkManager/conf.d/99-firewall-backend.conf** file with the following content:

```
[main]
firewall-backend=nftables
```

2. Reload the **NetworkManager** service.

```
# systemctl reload NetworkManager
```

(BZ#1548825)

firewalld rebased to version 0.9.3

The **firewalld** packages have been upgraded to upstream version 0.9.3, which provides a number of enhancements and bug fixes over the previous version.

For further details, see the upstream release notes:

- firewalld 0.9.3 Release Notes

- firewalld 0.9.2 Release Notes
- firewalld 0.8.6 Release Notes
- firewalld 0.8.5 Release Notes
- firewalld 0.8.4 Release Notes

(BZ#1872702)

4.8. KERNEL

Kernel version in RHEL 8.5 Beta

Red Hat Enterprise Linux 8.5 Beta is distributed with the kernel version 4.18.0-326.

(BZ#1839151)

IBM TSS 2.0 package rebased to 1.6.0

The IBM's Trusted Computing Group (TCG) Software Stack (TSS) 2.0 binary package has been upgraded to 1.6.0. This update adds the IBM TSS 2.0 support on AMD64 and Intel 64 architecture.

It is a user space TSS for Trusted Platform Modules (TPM) 2.0 and implements the functionality equivalent to (but not API compatible with) the TCG TSS working group's Enhanced System Application Interface (ESAPI), System Application Interface (SAPI), and TPM Command Transmission Interface (TCTI) API with a simpler interface.

It is a security middleware that allows applications and platforms to share and integrate the TPM into secure applications.

This rebase provides many bug fixes and enhancements over the previous version. The most notable changes include the following new attributes:

- **tsscertifyx509**: validates the **x509** certificate
- **tssgetcryptolibrary**: displays the current cryptographic library
- **tssprintattr**: prints the TPM attributes as text
- **tsspublicname**: calculates the public name of an entity
- **tsssetcommandcodeauditstatus**: clears or sets code via **TPM2_SetCommandCodeAuditStatus**
- **tsstpmcmd**: sends an in-band TPM simulator signal

(BZ#1822073)

The schedutil CPU frequency governor is now available on RHEL 8

The **schedutil** CPU governor uses CPU utilization data available on the CPU scheduler. **schedutil** is a part of the CPU scheduler and it can access the scheduler's internal data structures directly. **schedutil** controls how the CPU would raise and lower its frequency in response to system load. You must manually select the **schedutil** frequency governor as it is not enabled as default.

There is one **policyX** directory per CPU. **schedutil** is available in the **policyX/`scaling_governors** list of the existing **CPUFreq** governors in the kernel and is attached to **/sys/devices/system/cpu/cpufreq/policyx** policy. The policy file can be overwritten to change it.

Note that when using **intel_pstate** scaling drivers, it might be necessary to configure the **intel_pstate=passive** command line argument for **intel_pstate** to become available and be listed by the governor. **intel_pstate** is the default on Intel hardware with any modern CPU.

(BZ#1938339)

The rt-tests suite rebased to rt-tests-2.1 upstream version

The **rt-tests** suite has been rebased to **rt-tests-2.1** version, which provides multiple bug fixes and enhancements. The notable changes over the previous version include:

- Fixes to various programs in the **rt-tests** suite.
- Fixes to make programs more uniform with the common set of options, for example, the **oslat** program's option **-t --runtime** option is renamed to **-D** to specify the run duration to match the rest of the suite.
- Implements a new feature to output data in **json** format.

(BZ#1954387)

Intel® QuickAssist Technology Library (QATlib) was rebased to version 21.05

The **qatlib** package has been rebased to version 21.05, which provides multiple bug fixes and enhancements. Notable changes include:

- Adding support for several encryption algorithms:
  - AES-CCM 192/256
  - ChaCha20-Poly1305
  - PKE 8K (RSA, DH, ModExp, ModInv)
- Fixing device enumeration on different nodes
- Fixing **pci_vfio_set_command** for 32-bit builds

For more information about QATlib installation, check Ensuring that Intel® QuickAssist Technology stack is working correctly on RHEL 8.

(BZ#1920237)

The igc driver is now fully supported

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

(BZ#1495358)

vmcore capture fails after CPU hot-add or hot-removal operations

Previously, on IBM POWER systems, after every CPU or memory hot-plug or removal operation, the CPU data on the device tree became stale unless the **kdump.service** is reloaded. To reload the latest

CPU information, the **kdump.service** parses through the device nodes to fetch the CPU information. However, some of the CPU nodes are already lost during its hot-removal. Consequently, a race condition between the **kdump.service** reload and a CPU **hot-removal** happens at the same time and this may cause the dump to fail. A subsequent crash might then not capture the **vmcore** file.

This update eliminates the need to reload the **kdump.service** after a CPU hot-plug and the **vmcore** capture works as expected in the described scenario.

Note: This enhancement works as expected for firmware-assisted dumps (**fadump**). In the case of standard **kdump**, the **kdump.service** reload takes place during the **hot-plug** operation.

(BZ#1922951)

The kdumpctl command now supports the new **kdumpctl estimate** utility

The **kdumpctl** command now supports the **kdumpctl estimate** utility. Based on the existing **kdump** configuration, **kdumpctl estimate** prints a suitable estimated value for **kdump** memory allocation.

The minimum size of the crash kernel may vary depending on the hardware and machine specifications. Hence, previously, it was difficult to estimate an accurate **crashkernel=** value.

With this update, the **kdumpctl estimate** utility provides an estimated value. This value is a best effort recommended estimate and can serve as a good reference to configure a feasible **crashkernel=** value.

(BZ#1879558)

4.9. FILE SYSTEMS AND STORAGE

-H option added to the **rpc.gssd** daemon and the **set-home** option added to the **/etc/nfs.conf** file

This patch adds the **-H** option to **rpc.gssd** and the **set-home** option into **/etc/nfs.conf**, but does not change the default behavior.

By default, **rpc.gssd** sets **$HOME** to / to avoid possible deadlock that may happen when users' home directories are on an NFS share with Kerberos security. If either the **-H** option is added to **rpc.gssd**, or **set-home=0** is added to **/etc/nfs.conf**, **rpc.gssd** does not set **$HOME** to /.

These options allow you to use Kerberos k5identity files in **$HOME/.k5identity** and assumes NFS home directory is not on an NFS share with Kerberos security. These options are provided for use in only specific environments, such as the need for k5identity files. For more information see the **k5identity** man page.

(BZ#1868087)

xfs_quota state command now outputs all grace times when multiple quota types are specified

The **xfs_quota state** command now outputs grace times for multiple quota types specified on the command line. Previously, only one was shown even if more than one of **-g**, **-p**, or **-u** was specified.

(BZ#1949743)

The **storage** RHEL System Role now supports LVM VDO volumes

Virtual Data Optimizer (VDO) helps to optimize usage of the storage volumes. With this enhancement, administrators can use the **storage** System Role to manage **compression** and **deduplication** on Logical Manager Volumes (LVM) VDO volumes.

(BZ#1882475)

4.10. HIGH AVAILABILITY AND CLUSTERS

Local mode version of **pcs cluster setup** command is now fully supported

By default, the **pcs cluster setup** command automatically synchronizes all configuration files to the cluster nodes. Since RHEL 8.3, the **pcs cluster setup** command has provided the **--corosync-conf** option as a Technology Preview. This feature is now fully supported in RHEL 8.5. Specifying this option switches the command to **local** mode. In this mode, the **pcs** command-line interface creates a **corosync.conf** file and saves it to a specified file on the local node only, without communicating with any other node. This allows you to create a **corosync.conf** file in a script and handle that file by means of the script.

(BZ#1839637)

Ability to configure watchdog-only SBD for fencing on subset of cluster nodes

Previously, to use a watchdog-only SBD configuration, all nodes in the cluster had to use SBD. That prevented using SBD in a cluster where some nodes support it but other nodes (often remote nodes) required some other form of fencing. Users can now configure a watchdog-only SBD setup using the new **fence_watchdog** agent, which allows cluster configurations where only some nodes use watchdog-only SBD for fencing and other nodes use other fencing types. A cluster may only have a single such device, and it must be named **watchdog**.

(BZ#1443666)

New pcs command to update SCSI fencing device without causing restart of all other resources

Updating a SCSI fencing device with the **pcs stonith update** command causes a restart of all resources running on the same node where the stonith resource was running. The new **pcs stonith update-scsi-devices** command allows you to update SCSI devices without causing a restart of other cluster resources.

(BZ#1872378)

New reduced output display option for **pcs resource safe-disable** command

The **pcs resource safe-disable** and **pcs resource disable --safe** commands print a lengthy simulation result after an error report. You can now specify the **--brief** option for those commands to print errors only. The error report now always contains resource IDs of affected resources.

(BZ#1909901)

pcs now accepts **Promoted** and **Unpromoted** as role names

The **pcs** command-line interface now accepts **Promoted** and **Unpromoted** anywhere roles are specified in Pacemaker configuration. These role names are the functional equivalent of the **Master** and **Slave** Pacemaker roles. **Master** and **Slave** remain the names for these roles in configuration displays and help text.

(BZ#1885293)

New pcs resource status display commands

The **pcs resource status** and the **pcs stonith status** commands now support the following options:

- You can display the status of resources configured on a specific node with the **pcs resource status node=*node_id*** command and the **pcs stonith status node=*node_id*** command. You can use these commands to display the status of resources on both cluster and remote nodes.

- You can display the status of a single resource with the **pcs resource status *resource_id*** and the **pcs stonith status *resource_id*** commands.

- You can display the status of all resources with a specified tag with the **pcs resource status *tag_id*** and the **pcs stonith status *tag_id*** commands.

(BZ#1290830, BZ#1285269)

New LVM volume group flag to control autoactivation

LVM volume groups now support a **setautoactivation** flag which controls whether logical volumes that you create from a volume group will be automatically activated on startup. When creating a volume group that will be managed by Pacemaker in a cluster, set this flag to **n** with the **vgcreate --setautoactivation n** command for the volume group to prevent possible data corruption. If you have an existing volume group used in a Pacemaker cluster, set the flag with **vgchange --setautoactivation n**.

(BZ#1899214)

4.11. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS

A new module stream: ruby:3.0

RHEL 8.5 introduces **Ruby 3.0.2** in a new **ruby:3.0** module stream. This version provides a number of performance improvements, bug and security fixes, and new features over **Ruby 2.7** distributed with RHEL 8.3.

Notable enhancements include:

- Concurrency and parallelism features:
    - **Ractor**, an Actor-model abstraction that provides thread-safe parallel execution, is provided as an experimental feature.
    - **Fiber Scheduler** has been introduced as an experimental feature. **Fiber Scheduler** intercepts blocking operations, which enables light-weight concurrency without changing existing code.
- Static analysis features:
    - The **RBS** language has been introduced, which describes the structure of **Ruby** programs. The **rbs** gem has been added to parse type definitions written in **RBS**.
    - The **TypeProf** utility has been introduced, which is a type analysis tool for **Ruby** code.
- Pattern matching with the **case/in** expression is no longer experimental.
- One-line pattern matching, which is an experimental feature, has been redesigned.

- Find pattern has been added as an experimental feature.

The following performance improvements have been implemented:

- Pasting long code to the **Interactive Ruby Shell (IRB)** is now significantly faster.
- The **measure** command has been added to **IRB** for time measurement.

Other notable changes include:

- Keyword arguments have been separated from other arguments.
- The default directory for user-installed gems is now **$HOME/.local/share/gem/** unless the **$HOME/.gem/** directory is already present.

To install the **ruby:3.0** module stream, use:

```
# yum module install ruby:3.0
```

If you want to upgrade from an earlier **ruby** module stream, see Switching to a later stream.

(BZ#1938942)

Changes in the default separator for the Python urllib parsing functions

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

This change was implemented in Python 3.6 with the release of RHEL 8.4, and now is being backported to Python 3.8 and Python 2.7.

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

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

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

(BZ#1935686, BZ#1931555, BZ#1969517)

The Python ipaddress module no longer allows zeros in IPv4 addresses

To mitigate CVE-2021-29921, the Python **ipaddress** module now rejects IPv4 addresses with leading zeros with an **AddressValueError: Leading zeros are not permitted** error.

This change has been introduced in the **python38** and **python39** modules. Earlier Python versions distributed in RHEL are not affected by CVE-2021-29921.

Customers who rely on the previous behavior can pre-process their IPv4 address inputs to strip the leading zeros off. For example:

```
>>> def reformat_ip(address): return '.'.join(part.lstrip('0') if part != '0' else part for part in
address.split('.'))
>>> reformat_ip('0127.0.0.1')
'127.0.0.1'
```

To strip the leading zeros off with an explicit loop for readability, use:

```
def reformat_ip(address):
    parts = []
    for part in address.split('.'):
        if part != "0":
            part = part.lstrip('0')
        parts.append(part)
    return '.'.join(parts)
```

(BZ#1986007, BZ#1970504, BZ#1970505)

The php:7.4 module stream rebased to version 7.4.19

The PHP scripting language, provided by the **php:7.4** module stream, has been upgraded from version 7.4.6 to version 7.4.19. This update provides multiple security and bug fixes.

(BZ#1944110)

A new package: pg_repack

A new **pg_repack** package has been added to the **postgresql:12** and **postgresql:13** module streams. The **pg_repack** package provides a **PostgreSQL** extension that lets you remove bloat from tables and indexes, and optionally restore physical order of clustered indexes.

(BZ#1967193, BZ#1935889)

A new module stream: nginx:1.20

The **nginx 1.20** web and proxy server is now available as the **nginx:1.20** module stream. This update provides a number of bug fixes, security fixes, new features, and enhancements over the previously released version 1.18.

New features:

- **nginx** now supports client SSL certificate validation with Online Certificate Status Protocol (OCSP).
- **nginx** now supports cache clearing based on the minimum amount of free space. This support is implemented as the **min_free** parameter of the **proxy_cache_path** directive.
- A new **ngx_stream_set_module** module has been added, which enables you to set a value for a variable.

Enhanced directives:

- Multiple new directives are now available, such as **ssl_conf_command** and **ssl_reject_handshake**.
- The **proxy_cookie_flags** directive now supports variables.

Improved support for HTTP/2:

- The **ngx_http_v2** module now includes the **lingering_close**, **lingering_time**, **lingering_timeout** directives.

- Handling connections in HTTP/2 has been aligned with HTTP/1.x. From **nginx 1.20**, use the **keepalive_timeout** and **keepalive_requests** directives instead of the removed **http2_recv_timeout**, **http2_idle_timeout**, and **http2_max_requests** directives.

To install the **nginx:1.20** stream, use:

```
# yum module install nginx:1.20
```

If you want to upgrade from the **nginx:1.20** stream, see Switching to a later stream .

(BZ#1945671)

The squid:4 module stream rebased to version 4.15

The **Squid** proxy server, available in the **squid:4** module stream, has been upgraded from version 4.11 to version 4.15. This update provides various bug and security fixes.

(BZ#1964384)

quota now supports HPE XFS

The **quota** utilities now provide support for the HPE XFS file system. As a result, users of HPE XFS can monitor and and manage user and group disk usage through **quota** utilities.

(BZ#1945408)

mutt rebased to version 2.0.7

The **Mutt** email client has been updated to version 2.0.7, which provides a number of enhancements and bug fixes.

Notable changes include:

- **Mutt** now provides support for the **OAuth 2.0** authorization protocol using the **XOAUTH2** mechanism. Mutt now also supports the **OAUTHBEARER** authentication mechanism for the IMAP, POP, and SMTP protocols. The OAuth-based functionality is provided through external scripts. As a result, you can connect **Mutt** with various cloud email providers, such as **Gmail** using authentication tokens. For more information on how to set up **Mutt** with OAuth support, see How to set up Mutt with Gmail using OAuth2 authentication .

- **Mutt** adds support for domain-literal email addresses, for example, **user@[IPv6:fcXX:...]**.

- The new **$ssl_use_tlsv1_3** configuration variable allows TLS 1.3 connections if they are supported by the email server. This variable is enabled by default.

- The new **$imap_deflate** variable adds support for the **COMPRESS=DEFLATE** compression. The variable is disabled by default.

- The **$ssl_starttls** variable no longer controls aborting an unencrypted IMAP **PREAUTH** connection. Use the **$ssl_force_tls** variable instead if you rely on the **STARTTLS** process.

Note that even after an update to the new **Mutt** version, the **ssl_force_tls** configuration variable still defaults to **no** to prevent RHEL users from encountering problems in their existing environments. In the upstream version of **Mutt**, **ssl_force_tls** is now enabled by default.

(BZ#1912614, BZ#1890084)

4.12. COMPILERS AND DEVELOPMENT TOOLS

Go Toolset rebased to version 1.16.7

Go Toolset has been upgraded to version 1.16.7. Notable changes include:

- The **GO111MODULE** environment variable is now set to **on** by default. To revert this setting, change **GO111MODULE** to **auto**.
- The Go linker now uses less resources and improves code robustness and maintainability. This applies to all supported architectures and operating systems.
- With the new **embed** package you can access embedded files while compiling programs.
- All functions of the **io/ioutil** package have been moved to the **io** and **os** packages. While you can still use **io/ioutil**, the **io** and **os** packages provide better definitions.
- The Delve debugger has been rebased to 1.6.0 and now supports Go 1.16.7 Toolset.

(BZ#1938071)

Rust Toolset rebased to version 1.54.0

Rust Toolset has been updated to version 1.54.0. Notable changes include:

- The Rust standard library is now available for the **wasm32-unknown-unknown** target. With this enhancement, you can generate WebAssembly binaries, including newly stabilized intrinsics.
- Rust now includes the **IntoIterator** implementation for arrays. With this enhancement, you can use the **IntoIterator** trait to iterate over arrays by value and pass arrays to methods. However, **array.into_iter()** still iterates values by reference until the 2021 edition of Rust.
- The syntax for **or** patterns now allows nesting anywhere in the pattern. For example: **Pattern(1|2)** instead of **Pattern(1)|Pattern(2)**.
- Unicode identifiers can now contain all valid identifier characters as defined in the Unicode Standard Annex #31.
- Methods and trait implementations have been stabilized.
- Incremental compilation is re-enabled by default.

(BZ#1945805)

LLVM Toolset rebased to version 12.0.1

LLVM Toolset has been upgraded to version 12.0.1. Notable changes include:

- The new compiler flag **-march=x86-64-v[234]** has been added.
- The compiler flag **-fasynchronous-unwind-tables** of the **clang** compiler is now the default on Linux AArch64/PowerPC.
- The **clang** compiler now supports the C++20 likelihood attributes and .

- The new function attribute **tune-cpu** has been added. It allows microarchitectural optimizations to be applied independently from the **target-cpu** attribute or TargetMachine CPU.
- The new sanitizer **-fsanitize=unsigned-shift-base** has been added to the integer sanitizer **-fsanitize=integer** to improve security.
- Code generation on PowerPC targets has been optimized.
- The WebAssembly backend is now enabled in LLVM. With this enhancement, you can generate WebAssembly binaries with LLVM and Clang.
- For debugging .NET applications, use the lldb debugger. For other languages, use the gdb debugger.

(BZ#1927937)

CMake rebased to version 3.20.2

CMake has been rebased from 3.18.2 to 3.20.2. To use CMake on a project that requires the version 3.20.2 or less, use the command cmake_minimum_required(version 3.20.2).

Notable changes include:

- C++23 compiler modes can now be specified by using the target properties **CXX_STANDARD**, **CUDA_STANDARD**, **OBJCXX_STANDARD**, or by using the **cxx_std_23** meta-feature of the compile features function.
- CUDA language support now allows the NVIDIA CUDA compiler to be a symbolic link.
- The Intel oneAPI NextGen LLVM compilers are now supported with the **IntelLLVM** compiler ID .
- CMake now facilitates cross compiling for Android by merging with the Android NDK's toolchain file.
- When running **cmake(1)** to generate a project build system, unknown command-line arguments starting with a hyphen are now rejected.

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

(BZ#1957947)

New GCC Toolset 11

GCC Toolset 11 is a compiler toolset that provides recent versions of development tools. It is available as an Application Stream in the form of a Software Collection in the **AppStream** repository.

The following components have been rebased since GCC Toolset 10:

- GCC to version 11.1.1
- GDB to version 10.1
- Valgrind to version 3.17.0
- SystemTap to version 4.5
- **binutils** to version 2.36.1
- **elfutils** to version 0.184

- **dwz** to version 0.14
- Annobin to version 9.69

To install GCC Toolset 11, run the following command as root:

```
# yum install gcc-toolset-11
```

To run a tool from GCC Toolset 11:

```
$ scl enable gcc-toolset-11 tool
```

To run a shell session where tool versions from GCC Toolset 11 override system versions of these tools:

```
$ scl enable gcc-toolset-11 bash
```

For more information, see Using GCC Toolset.

The GCC Toolset 11 components are also available in the two container images:

- **rhel8/gcc-toolset-11-toolchain**, which includes the GCC compiler, the GDB debugger, and the **make** automation tool.
- **rhel8/gcc-toolset-11-perftools**, which includes the performance monitoring tools, such as SystemTap and Valgrind.

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

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

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

(BZ#1953094)

GCC Toolset 11: dwz now supports DWARF 5

In GCC Toolset 11, the **dwz** tool now supports the DWARF Version 5 debugging format.

(BZ#1948709)

SystemTap rebased to version 4.5

The SystemTap package has been updated to version 4.5. Notable bug fixes and enhancements include:

- 32-bit floating-point variables are automatically widened to double variables and, as a result, can be accessed directly as **$context** variables.
- **enum** values can be accessed as **$context** variables.
- The BPF uconversions tapset has been extended and includes more tapset functions to access values in user space, for example **user_long_error()**.
- Concurrency control has been significantly improved to provide stable operation on large servers.

For further information, see the upstream SystemTap 4.5 release notes.

(BZ#1933889)

elfutils rebased to version 0.185

The **elfutils** package has been updated to version 0.185. Notable bug fixes and enhancements include:

- The **eu-elflint** and **eu-readelf** tools now recognize and show the **SHF_GNU_RETAIN** and **SHT_X86_64_UNWIND** flags on ELF sections.
- The **DEBUGINFOD_SONAME** macro has been added to **debuginfod.h**. This macro can be used with the **dlopen** function to load the **libdebuginfod.so** library dynamically from an application.
- A new function **debuginfod_set_verbose_fd** has been added to the **debuginfod-client** library. This function enhances the **debuginfod_find_*** queries functionality by redirecting the verbose output to a separate file.
- Setting the **DEBUGINFOD_VERBOSE** environment variable now shows more information about which servers the **debuginfod** client connects to and the HTTP responses of those servers.
- The **debuginfod** server provides a new thread-busy metric and more detailed error metrics to make it easier to inspect processes that run on the **debuginfod** server.
- The **libdw** library now transparently handles the **DW_FORM_indirect** location value so that the **dwarf_whatform** function returns the actual FORM of an attribute.
- To reduce network traffic, the **debuginfod-client** library stores negative results in a cache, and client objects can reuse an existing connection.

(BZ#1933890)

Valgrind rebased to version 3.17.0

The Valgrind package has been updated to version 3.17.0. Notable bug fixes and enhancements include:

- Valgrind can read the DWARF Version 5 debugging format.
- Valgrind supports debugging queries to the **debuginfod** server.
- The ARMv8.2 processor instructions are partially supported.
- The Power ISA v.3.1 instructions on POWER10 processors are partially supported.
- The IBM z14 processor instructions are supported.
- Most IBM z15 instructions are supported. The Valgrind tool suite supports the miscellaneous-instruction-extensions facility 3 and the vector-enhancements facility 2 for the IBM z15 processor. As a result, Valgrind runs programs compiled with GCC **-march=z15** correctly and provides improved performance and debugging experience.
- The **--track-fds=yes option** respects **-q** (**--quiet**) and ignores the standard file descriptors **stdin**, **stdout**, and **stderr** by default. To track the standard file descriptors, use the **--track-fds=all** option.
- The DHAT tool has two new modes of operation: **--mode=copy** and **--mode=ad-hoc**.

(BZ#1933891)

DAWR functionality improved in GDB on IBM POWER10

With this enhancement, new hardware watchpoint capabilities are now enabled for GDB on the IBM POWER10 processors. For example, a new set of DAWR/DAWRX registers has been added.

(BZ#1854784)

PAPI library support for Fujitsu A64FX added

PAPI library support for Fujitsu A64FX has been added. With this feature, developers can collect hardware statistics.

(BZ#1908126)

The PCP package was rebased to 5.3.1

The Performance Co-Pilot (PCP) package has been rebased to version 5.3.1. This release includes bug fixes, enhancements, and new features. Notable changes include:

- Scalability improvements, which now support centrally logged performance metrics for hundreds of hosts (**pmlogger** farms) and automatic monitoring with performance rules (**pmie** farms).
- Resolved memory leaks in the **pmproxy** service and the **libpcp_web** API library, and added instrumentation and new metrics to **pmproxy**.
- A new **pcp-ss** tool for historical socket statistics.
- Improvements to the **pcp-htop** tool.
- Extensions to the over-the-wire PCP protocol which now support higher resolution timestamps.

(BZ#1922040)

The grafana package was rebased to version 7.5.9

The **grafana** package has been rebased to version 7.5.9. Notable changes include:

- New time series panel (beta)
- New pie chart panel (beta)
- Alerting support for Loki
- Multiple new query transformations

For more information, see What’s New in Grafana v7.4 , What’s New in Grafana v7.5 .

(BZ#1921191)

The grafana-pcp package was rebased to 3.1.0

The **grafana-pcp** package has been rebased to version 3.1.0. Notable changes include:

- Performance Co-Pilot (PCP) Vector Checklist dashboards use a new time series panel, show units in graphs, and contain updated help texts.
- Adding **pmproxy** URL and **hostspec** variables to PCP Vector Host Overview and PCP Checklist dashboards.

- All dashboards display datasource selection.
- Marking all included dashboards as readonly.
- Adding compatibility with Grafana 8.

(BZ#1921190)

grafana-container rebased to version 7.5.9

The **rhel8/grafana** container image provides Grafana. Notable changes include:

- The **grafana** package is now updated to version 7.5.9.
- The **grafana-pcp** package is now updated to version 3.1.0.
- The container now supports the **GF_INSTALL_PLUGINS** environment variable to install custom Grafana plugins at container startup

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

To pull this container image, execute the following command:

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

(BZ#1971557)

pcp-container rebased to version 5.3.1

The **rhel8/pcp** container image provides Performance Co-Pilot. The **pcp-container** package has been upgraded to version 5.3.1. Notable changes include:

- The **pcp** package is now updated to version 5.3.1.

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

To pull this container image, execute the following command:

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

(BZ#1974912)

The new **pcp-ss** PCP utility is now available.

The **pcp-ss** PCP utility reports socket statistics collected by the **pmdasockets(1)** PMDA. The command is compatible with many of the **ss** command line options and reporting formats. It also offers the advantages of local or remote monitoring in live mode and historical replay from a previously recorded PCP archive.

(BZ#1879350)

4.13. IDENTITY MANAGEMENT

IdM now supports new password policy options

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

--maxrepeat

Specifies the maximum number of the same character in sequence.

--maxsequence

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

--dictcheck

Checks if the password is a dictionary word.

--usercheck

Checks if the password contains the username.

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

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

(JIRA:RHELPLAN-89566)

Improved the SSSD debug logging by adding a unique identifier tag for each request

As SSSD processes requests asynchronously, it is not easy to follow log entries for individual requests in the backend logs, as messages from different requests are added to the same log file. To improve the readability of debug logs, a unique request identifier is now added to log messages in the form of **RID# <integer>**. This allows you to isolate logs pertaining to an individual request, and you can track requests from start to finish across log files from multiple SSSD components.

For example, the following sample output from an SSSD log file shows the unique identifiers RID#3 and RID#4 for two different requests:

```
(2021-07-26 18:26:37): [be[testidm.com]] [dp_req_destructor] (0x0400): RID#3 Number of active DP
request: 0
(2021-07-26 18:26:37): [be[testidm.com]] [dp_req_reply_std] (0x1000): RID#3 DP Request
AccountDomain #3: Returning [Internal Error]: 3,1432158301,GetAccountDomain() not supported
(2021-07-26 18:26:37): [be[testidm.com]] [dp_attach_req] (0x0400): RID#4 DP Request Account #4:
REQ_TRACE: New request. sssd.nss CID #1 Flags [0x0001].
(2021-07-26 18:26:37): [be[testidm.com]] [dp_attach_req] (0x0400): RID#4 Number of active DP
request: 1
```

(JIRA:RHELPLAN-92473)

samba rebased to version 4.14.4

The *samba* packages have been upgraded to upstream version 4.14.4, which provides bug fixes and enhancements over the previous version:

- Publishing printers in Active Directory (AD) has increased reliability, and additional printer features have been added to the published information in AD. Also, Samba now supports Windows drivers for the ARM64 architecture.

- The **ctdb isnotrecmaster** command has been removed. As an alternative, use **ctdb pnn** or the **ctdb recmaster** commands.

- The clustered trivial database (CTDB) **ctdb natgw master** and **slave-only** parameters have been renamed to **ctdb natgw leader** and **follower-only**.

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

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

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

(BZ#1944657)

The dnaInterval configuration attribute is now supported

With this update, Red Hat Directory Server supports setting the **dnaInterval** attribute of the Distributed Numeric Assignment (DNA) plug-in in the **cn=*<DNA_config_entry>*,cn=Distributed Numeric Assignment Plugin,cn=plugins,cn=config** entry. The DNA plug-in generates unique values for specified attributes. In a replication environment, servers can share the same range. To avoid overlaps on different servers, you can set the **dnaInterval** attribute to skip some values. For example, if the interval is **3** and the first number in the range is **1**, the next number used in the range is **4**, then **7**, then **10**.

For further details, see the dnaInterval parameter description.

(BZ#1938239)

Directory Server rebased to version 1.4.3.23

The **389-ds-base** packages have been upgraded to upstream version 1.4.3.23, which provides a number of bug fixes and enhancements over the previous version. For a complete list of notable changes, read the upstream release notes before updating:

- https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-3-23.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-3-22.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-3-21.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-3-20.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-3-19.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-3-18.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-3-17.html

(BZ#1947044)

Directory Server now supports temporary passwords

This enhancement enables administrators to configure temporary password rules in global and local password policies. With these rules, you can configure that, when an administrator resets the password of a user, the password is temporary and only valid for a specific time and for a defined number of attempts. Additionally, you can configure that the expiration time does not start directly when the administrator changes the password. As a result, Directory Server allows the user only to authenticate using the temporary password for a finite period of time or attempts. Once the user authenticates successfully, Directory Server allows this user only to change its password.

(BZ#1626633)

Directory Server provides monitoring settings that can prevent database corruption caused by lock exhaustion

This update adds the **nsslapd-db-locks-monitoring-enable** parameter to the **cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config** entry. If it is enabled, which is the default, Directory Server aborts all of the searches if the number of active database locks is higher than the percentage threshold configured in **nsslapd-db-locks-monitoring-threshold**. If an issue is encountered, the administrator can increase the number of database locks in the **nsslapd-db-locks** parameter in the **cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config** entry. This can prevent data corruption. Additionally, the administrator now can set a time interval in milliseconds that the thread sleeps between the checks.

For further details, see the parameter descriptions in the Red Hat Directory Server Configuration, Command, and File Reference.

(BZ#1812286)

Directory Server can exclude attributes and suffixes from the retro changelog database

This enhancement adds the **nsslapd-exclude-attrs** and **nsslapd-exclude-suffix** parameters to Directory Server. You can set these parameters in the **cn=Retro Changelog Plugin,cn=plugins,cn=config** entry to exclude certain attributes or suffixes from the retro changelog database.

(BZ#1850664)

Directory Server supports the entryUUID attribute

With this enhancement, Directory Server supports the **entryUUID** attribute to be compliant with RFC 4530. For example, with support for **entryUUID**, migrations from OpenLDAP are easier. By default, Directory Server adds the **entryUUID** attribute only to new entries. To manually add it to existing entries, use the **dsconf *<instance_name>* plugin entryuuid fixup** command.

(BZ#1944494)

4.14. DESKTOP

You can now connect to network at the login screen

With this update, you can now connect to your network and configure certain network options at the GNOME Display Manager (GDM) login screen. As a result, you can log in as an enterprise user whose home directory is stored on a remote server.

The login screen supports the following network options:

- Wired network
- Wireless network, including networks protected by a password
- Virtual Private Network (VPN)

The login screen cannot open windows for additional network configuration. As a consequence, you cannot use the following network options at the login screen:

- Networks that open a captive portal

- Modem connections
- Wireless networks with enterprise WPA or WPA2 encryption that have not been preconfigured

The network options at the login screen are disabled by default. To enable the network settings, use the following procedure:

1. Create the **/etc/polkit-1/rules.d/org.gnome.gdm.rules** file with the following content:

```
polkit.addRule(function(action, subject) {
    if (action.id == "org.freedesktop.NetworkManager.network-control" &&
        subject.user == "gdm") {
            return polkit.Result.YES;
    }

    return polkit.Result.NOT_HANDLED;
});
```

2. Restart GDM:

```
# systemctl restart gdm
```

WARNING

Restarting GDM terminates all your graphical user sessions.

3. At the login screen, access the network settings in the menu on the right side of the top panel.

(BZ#1935261)

Displaying the system security classification at login

You can now configure the GNOME Display Manager (GDM) login screen to display an overlay banner that contains a predefined message. This is useful for deployments where the user is required to read the security classification of the system before logging in.

To enable the overlay banner and configure a security classification message, use the following procedure:

1. Install the **gnome-shell-extension-heads-up-display** package:

```
# yum install gnome-shell-extension-heads-up-display
```

2. Create the **/etc/dconf/db/gdm.d/99-hud-message** file with the following content:

```
[org/gnome/shell]
enabled-extensions=['heads-up-display@gnome-shell-extensions.gcampax.github.com']
```

```
[org/gnome/shell/extensions/heads-up-display]
message-heading="Security classification title"
message-body="Security classification description"
```

Replace the following values with text that describes the security classification of your system:

Security classification title

A short heading that identifies the security classification.

Security classification description

A longer message that provides additional details, such as references to various guidelines.

3. Update the **dconf** database:

   ```
   # dconf update
   ```

4. Reboot the system.

(BZ#1651378)

Flicker free boot is available

You can now enable flicker free boot on your system. When flicker free boot is enabled, it eliminates abrupt graphical transitions during the system boot process, and the display does not briefly turn off during boot.

To enable flicker free boot, use the following procedure:

1. Configure the boot loader menu to hide by default:

   ```
   # grub2-editenv - set menu_auto_hide=1
   ```

2. Update the boot loader configuration:

   - On UEFI systems:

     ```
     # grub2-mkconfig -o /etc/grub2-efi.cfg
     ```

   - On legacy BIOS systems:

     ```
     # grub2-mkconfig -o /etc/grub2.cfg
     ```

3. Reboot the system.

As a result, the boot loader menu does not display during system boot, and the boot process is graphically smooth.

To access the boot loader menu, repeatedly press **Esc** after turning on the system.

(JIRA:RHELPLAN-99148)

You can set a default desktop session for all users

With this update, you can now configure a default desktop session that is preselected for all users that have not logged in yet.

If a user logs in using a different session than the default, their selection persists to their next login.

To configure the default session, use the following procedure:

1. Copy the configuration file template:

   # cp /usr/share/accountsservice/user-templates/standard \ /etc/accountsservice/user-templates/standard ---

2. Edit the new **/etc/accountsservice/user-templates/standard** file. On the **Session=*gnome*** line, replace ***gnome*** with the session that you want to set as the default.

3. Optional: To configure an exception to the default session for a certain user, copy the template file to **/var/lib/AccountsService/users/*user-name*** and edit it there.

4. Reboot the system.

(BZ#1812788)

4.15. GRAPHICS INFRASTRUCTURES

Support for new GPUs

The following new GPUs are now supported:

Intel graphics

- Alder Lake-S (ADL-S)

Support for Alder Lake-S graphics is disabled by default. To enable it, add the following option to the kernel command line:

```
i915.force_probe=PCI_ID
```

Replace *PCI_ID* with either the PCI device ID of your Intel GPU, or with the ***** character to enable support for all alpha-quality hardware that uses the **i915** driver.

- Elkhart Lake (EHL)

- Comet Lake Refresh (CML-R) with the TGP Platform Controller Hub (PCH)

AMD graphics

- Cezzane and Barcelo

- Sienna Cichlid

- Dimgrey Cavefish

(JIRA:RHELPLAN-99040, BZ#1784132, BZ#1784136, BZ#1838558)

The Wayland session is available with the proprietary NVIDIA driver

The proprietary NVIDIA driver now supports hardware accelerated OpenGL and Vulkan rendering in Xwayland. As a result, you can now enable the GNOME Wayland session with the proprietary NVIDIA driver. Previously, only the legacy X11 session was available with the driver. X11 remains as the default session to avoid a possible disruption when updating from a previous version of RHEL.

To enable Wayland with the NVIDIA proprietary driver, use the following procedure:

1. Enable Direct Rendering Manager (DRM) kernel modesetting by adding the following option to the kernel command line:

   ```
   nvidia-drm.modeset=1
   ```

   For details on enabling kernel options, see Configuring kernel command-line parameters.

2. Reboot the system.
   The Wayland session is now available at the login screen.

3. Optional: To avoid the loss of video allocations when suspending or hibernating the system, enable the power management option with the driver. For details, see Configuring Power Management Support.

For the limitations related to the use of DRM kernel modesetting in the proprietary NVIDIA driver, see Direct Rendering Manager Kernel Modesetting (DRM KMS) .

(JIRA:RHELPLAN-99049)

Improvements to GPU support

The following new GPU features are now enabled:

- Panel Self Refresh (PSR) is now enabled for Intel Tiger Lake and later graphics, which improves power consumption.

- Intel Tiger Lake, Ice Lake, and later graphics can now use High Bit Rate 3 (HBR3) mode with the DisplayPort Multi-Stream Transport (DP-MST) transmission method. This enables support for certain display capabilities with docks.

- Modesetting is now enabled on NVIDIA Ampere GPUs. This includes the following models: GA102, GA104, and GA107, including hybrid graphics systems.

- Most laptops with Intel integrated graphics and an NVIDIA Ampere GPU can now output to external displays using either GPU.

(JIRA:RHELPLAN-99043)

Updated graphics drivers

The following graphics drivers have been updated:

- **amdgpu**
- **ast**
- **i915**
- **mgag2000**
- **nouveau**
- **vmwgfx**

- **vmwgfx**
- The Mesa library
- Vulkan packages

(JIRA:RHELPLAN-99044)

Intel Tiger Lake graphics are fully supported

Intel Tiger Lake UP3 and UP4 Xe graphics, which were previously available as a Technology Preview, are now fully supported. Hardware acceleration is enabled by default on these GPUs.

(BZ#1783396)

4.16. RED HAT ENTERPRISE LINUX SYSTEM ROLES

Users can configure the maximum root distance using the **timesync_max_distance** parameter

With this update, the **timesync** RHEL System Role is able to configure the **tos maxdist** of **ntpd** and the **maxdistance** parameter of the **chronyd** service using the new **timesync_max_distance** parameter. The **timesync_max_distance** parameter configures the maximum root distance to accept measurements from Network Time Protocol (NTP) servers. The default value is 0, which keeps the provider-specific defaults.

(BZ#1938016)

Elasticsearch can now accept lists of servers

Previously, the **server_host** parameter accepted only a string value for a single host. With this enhancement, it also accepts a list of strings to support multiple hosts. As a result, you can now configure multiple Elasticsearch hosts in one Elasticsearch output dictionary.

(BZ#1986463)

Network Time Security (NTS) option added to the **timesync** RHEL System Role

The **nts** option was added to the **timesync** RHEL System Role to enable NTS on client servers. NTS is a new security mechanism specified for Network Time Protocol (NTP), which can secure synchronization of NTP clients without client-specific configuration and can scale to large numbers of clients. The **NTS** option is supported only with the **chrony** NTP provider in version 4.0 and later.

(BZ#1970664)

The **sshd** RHEL System Role now supports non-exclusive configuration snippets

This enhancement enables you to configure **sshd** from different roles or playbooks without rewriting each other’s results. For that, you can use namespaces. They are similar to a drop-in directory, which can define non-exclusive configuration snippets for **sshd**. As a result, the **sshd** RHEL System Role can be used from different roles, if they need just a configuration snippet and not a control of the content of the whole configuration file.

(BZ#1970642)

The **SELinux** role can now manage SELinux modules

The **SElinux** RHEL System Role has the ability to manage SELinux modules. With this update, users can provide their own custom modules from **.pp** or **.cil** files, which allows for a more flexible SELinux policy management.

(BZ#1848683)

ha_cluster role now supports pacemaker cluster configuration

With this update, you can use the **ha_cluster** role to configure a basic corosync cluster and pacemaker cluster properties, stonith and resources.

(BZ#1963283)

Users can manage the chrony interleaved mode, NTP filtering, and hardware timestamping

With this update, the **timesync** RHEL System Role enables you to configure the Network Time Protocol (NTP) interleaved mode, additional filtering of NTP measurements, and hardware timestamping. The **chrony** package of version 4.0 adds support for these functionalities to achieve a highly accurate and stable synchronization of clocks in local networks.

- To enable the NTP interleaved mode, make sure the server supports this feature, and set the **xleave** option to **yes** for the server in the **timesync_ntp_servers** list. The default value is **no**.
- To set the number of NTP measurements per clock update, set the **filter** option for the NTP server you are configuring. The default value is **1**.
- To set the list of interfaces which should have hardware timestamping enabled for NTP, use the **timesync_ntp_hwts_interfaces** parameter. The special value **["*"]** enables timestamping on all interfaces that support it. The default is **[]**.

(BZ#1938020)

timesync role enables customization settings for chrony

Previously, there was no way to provide customized chrony configuration using the **timesync** role. This update adds the **timesync_chrony_custom_settings** parameter, which enables users to to provide customized settings for chrony, such as:

```
timesync_chrony_custom_settings:
  - "logdir /var/log/chrony"
  - "log measurements statistics tracking"
```

(BZ#1938023)

timesync role supports hybrid end-to-end delay mechanisms

With this enhancement, you can use the new **hybrid_e2e option** in **timesync_ptp_domains** to enable hybrid end-to-end delay mechanisms in the **timesync** role. The hybrid end-to-end delay mechanism uses unicast delay requests, which are useful to reduce multicast traffic in large networks.

(BZ#1957849)

ethtool now supports reducing the packet loss rate and latency

Tx or Rx buffers are memory spaces allocated by a network adapter to handle traffic bursts. Properly managing the size of these buffers is critical to reduce the packet loss rate and achieve acceptable network latency.

The **ethtool** utility now reduces the packet loss rate or latency by configuring the **ring** option of the specified network device.

The list of supported **ring** parameters is:

- **rx** - Changes the number of ring entries for the Rx ring.
- **rx-jumbo** - Changes the number of ring entries for the Rx Jumbo ring.
- **rx-mini** - Changes the number of ring entries for the Rx Mini ring.
- **tx** - Changes the number of ring entries for the Tx ring.

(BZ#1959649)

New **ipv6_disabled** parameter is now available

With this update, you can now use the **ipv6_disabled** parameter to disable ipv6 when configuring addresses.

(BZ#1939711)

RHEL System Roles now supports VPN management

Previously, it was difficult to set up secure and properly configured IPsec tunneling and virtual private networking (VPN) solutions on Linux. With this enhancement, you can use the VPN RHEL System Role to set up and configure VPN tunnels for host-to-host and mesh connections more easily across large numbers of hosts. As a result, you have a consistent and stable configuration interface for VPN and IPsec tunneling configuration within the RHEL System Roles project.

(BZ#1943679)

The **storage** RHEL System Role now supports **filesystem** relabel

Previously, the **storage** role did not support relabelling. This update fixes the issue, providing support to relabel the **filesystem** label. To do this, set a new label string to the **fs_label** parameter in **storage_volumes**.

(BZ#1876315)

Support for volume sizes expressed as a percentage is available in the **storage** System Role

This enhancement adds support to the **storage** RHEL System Role to express LVM volume sizes as a percentage of the pool's total size. You can specify the size of LVM volumes as a percentage of the pool/VG size, for example: **50%** in addition to the human-readable size of the file system, for example, **10g**, **50 GiB**.

(BZ#1894642)

ha_cluster role now supports pacemaker cluster configuration

With this update, you can use the **ha_cluster** role to configure a basic corosync cluster and pacemaker cluster properties, stonith and resources.

(BZ#1978726)

New Ansible Role for Microsoft SQL Server Management

The new **microsoft.sql.server** role is designed to help IT and database administrators automate processes involved with setup, configuration, and performance tuning of SQL Server on Red Hat Enterprise Linux.

(BZ#2013853)

The postfix role of RHEL System Roles is fully supported

Red Hat Enterprise Linux System Roles provides a configuration interface for Red Hat Enterprise Linux subsystems, which makes system configuration easier through the inclusion of Ansible Roles. This interface enables managing system configurations across multiple versions of Red Hat Enterprise Linux, as well as adopting new major releases.

The **rhel-system-roles** packages are distributed through the AppStream repository.

As of RHEL 8.5, the **postfix** role is fully supported.

For more information, see the Knowledgebase article about RHEL System Roles.

(BZ#1812552)

4.17. RHEL IN CLOUD ENVIRONMENTS

RHEL on Azure now supports MANA

RHEL 8.5 and later virtual machines running on Microsoft Azure can now use the Microsoft Azure Network Adapter (MANA).

(BZ#1957820)

4.18. SUPPORTABILITY

sos rebased to version 4.1

The **sos** package has been upgraded to version 4.1, which provides multiple bug fixes and enhancements. Notable enhancements include:

- Red Hat Update Infrastructure (**RHUI**) plugin is now natively implemented in the **sos** package. With the **rhui-debug.py** python binary, **sos** can collect reports from **RHUI** including, for example, the main configuration file, the **rhui-manager** log file, or the installation configuration.

- **sos** introduces the **--cmd-timeout** global option that sets manually a timeout for a command execution. The default value (-1) defers to the general command timeout, which is 300 seconds.

(BZ#1928679)

CHAPTER 5. BUG FIXES

This part describes bugs fixed in Red Hat Enterprise Linux 8.5 Beta that have a significant impact on users.

5.1. INSTALLER AND IMAGE CREATION

RHEL-Edge container image now uses nginx and serves on port 8080

Previously, the **edge-container** image type was unable to run in non-root mode. As a result, Red Hat OpenShift 4 was unable to use the **edge-container** image type. With this enhancement, the container now uses **nginx** HTTP server to serve the commit and a configuration file that allows the server to run as a non-root user inside the container, enabling its use on Red Hat OpenShift 4. The internal web server now uses the port **8080** instead of **80**.

(BZ#1945238)

RHEL installation no longer aborts when Insights client fails to register system

Previously, the RHEL installation failed with an error at the end if the Red Hat Insights client failed to register the system during the installation. With this update, the system completes the installation even if the insights client fails. The user is notified about the error during installation so the error can be handled later independently.

(BZ#1931069)

5.2. SHELLS AND COMMAND-LINE TOOLS

opal-prd rebased to version 6.7.1

opal-prd has been upgraded to version 6.7.1. Notable bug fixes and enhancements include:

- Fixed **xscom** error logging issues caused due to **xscom OPAL** call.
- Fixed possible deadlock with the **DEBUG** build.
- Fallback to **full_reboot** if **fast-reboot** fails in **core/platform**.
- Fixed **next_ungarded_primary** in **core/cpu**.
- Improved rate limit timer requests and the timer state in Self-Boot Engine (SBE).

(BZ#1921665)

libservicelog rebased to version 1.1.19

libservicelog has been upgraded to version 1.1.19. Notable bug fixes and enhancements include:

- Fixed output alignment issue.
- Fixed **segfault** on **servicelog_open()** failure.

(BZ#1844430)

ipmitool sol activate command no longer crashes

Previously, after upgrading from RHEL 7 to RHEL 8 the **ipmitool sol activate** command would crash while trying to access the remote console on an IBM DataPower appliance.

With this update, the bug has been fixed and one can use **ipmitool** to access the remote console again.

(BZ#1951480)

Relax-and-Recover (ReaR) package now depends on the bootlist executable

Previously, ReaR could produce a rescue image without the bootlist executable on the IBM Power Systems, Little Endian architecture. Consequently, if the **powerpc-utils-core** package is not installed, the rescue image did not contain the bootlist executable.

With this update, the ReaR package now depends on the bootlist executable. The dependency ensures that the bootlist executable is present. ReaR does not create a rescue image if the bootlist executable is missing. This avoids creating an invalid rescue image.

(BZ#1983013)

rsync with an unprivileged remote user can now be used in ReaR

Previously, when rsync was used to back up and restore the system data **(BACKUP=RSYNC)**, the parameters to rsync were incorrectly quoted, and the **--fake-super** parameter was not passed to the remote rsync process. Consequently, the file metadata was not correctly saved and restored.

With this update following bugs have been fixed:

- ReaR uses the correct parameters for rsync.
- Improved rsync code for error detection during backup and restore:
    - If there is a rsync error detected during the backup, ReaR aborts with an error message.
    - If there is a rsync error detected during the restore, ReaR displays a warning message.

In the **/etc/rear/local.conf** file set **BACKUP_INTEGRITY_CHECK=1** to turn the warning into an error message.

(BZ#1930662)

Loss of backup data on network shares when using ReaR does not occur anymore

Previously, when a network file system like NFS was used to store the ReaR backups, in case of an error ReaR removed the directory where the NFS was mounted. Consequently, this caused backup data loss.

With this update, ReaR now uses a new method to unmount network shares. This new method does not remove the content of the mounted filesystem when it is removes the mount point. The loss of backup data on network shares when using ReaR is now fixed.

(BZ#1958247)

ReaR can now be used to back up and recover machines that use ESP

Previously, ReaR did not create Extensible Firmware Interface (EFI) entries when software RAID (MDRAID) is used for the EFI System Partition on machines with Unified Extensible Firmware Interface (UEFI) firmware. When a system with UEFI firmware and EFI System Partition on software RAID were recovered using ReaR; the recovered system was unbootable and required manual intervention to fix the boot EFI variables.

With this update, the support for creating boot EFI entries for software RAID devices is added to ReaR. ReaR can now be used to back up and recover machines that use EFI System Partition (ESP) on software RAID, without manual post-recovery intervention.

(BZ#1958222)

/etc/slp.spi file added to openslp package

Previously, the **/etc/slp.spi** file was missing in the **openslp** package. Consequently, the **/usr/bin/slptool** command did not generate output. With this update, **/etc/slp.spi** has been added to **openslp**.

(BZ#1965649)

BM Power Systems, Little Endian architecture machines with multipath can now be safely recovered using ReaR

Previously, the **/sys** file system was not mounted in the chroot when ReaR was recovering the system. The **ofpathname** executable on the IBM Power Systems, Little Endian architecture failed when installing the boot loader. Consequently, the error remained undetected and the recovered system was unbootable.

With this update, ReaR now mounts the **/sys** file system in the recovery chroot. ReaR ensures that **ofpathname** is present in the rescue system on Power Systems, Little Endian architecture machines.

(BZ#1983003)

5.3. INFRASTRUCTURE SERVICES

Permissions of the /var/lib/chrony have changed

Previously, enterprise security scanners would flag the **/var/lib/chrony** directory for having world-readable and executable permissions. With this update, the permissions of the **/var/lib/chrony** directory have changed to limit access only to the root and chrony users.

(BZ#1939295)

5.4. SECURITY

GnuTLS no longer rejects SHA-1-signed CAs if they are explicitly trusted

Previously, the **GnuTLS** library checked signature hash strength of all certificate authorities (CA) even if the CA was explicitly trusted. As a consequence, chains containing CAs signed with the SHA-1 algorithm were rejected with the error message **certificate's signature hash strength is unacceptable**. With this update, **GnuTLS** excludes trusted CAs from the signature hash strength checks and therefore no longer rejects certificate chains containing CAs even if they are signed using weak algorithms.

(BZ#1965445)

SELinux policy did not allow GDM to set the GRUB boot_success flag

Previously, SELinux policy did not allow the GNOME Display Manager (GDM) to set the GRUB **boot_success** flag during the power-off and reboot operations. Consequently, the GRUB menu appeared on the next boot. With this update, the SELinux policy introduces a new **xdm_exec_bootloader** boolean that allows the GDM to set the GRUB **boot_success** flag, and which is enabled by default. As a result, the GRUB boot menu is shown on the first boot and the flicker-free boot support feature works correctly.

(BZ#1994096)

OSCAP Anaconda Addon now handles customized profiles

Previously, the **OSCAP Anaconda Addon** plugin did not correctly handle security profiles with customizations in separate files. Consequently, the customized profiles were not available in the RHEL graphical installation even when you specified them in the corresponding Kickstart section. The handling has been fixed, and you can use customized SCAP profiles in the RHEL graphical installation.

(BZ#1691305)

OpenSCAP no longer fails during evaluation of the STIG profile and other SCAP content

Previously, initialization of the cryptography library in OpenSCAP was not performed properly in OpenSCAP, specifically in the **filehash58** probe. As a consequence, a segmentation fault occurred while evaluating SCAP content containing the **filehash58_test** Open Vulnerability Assessment Language (OVAL) test. This affected in particular the evaluation of the STIG profile for Red Hat Enterprise Linux 8. The evaluation failed unexpectedly and results were not generated. The process of initializing libraries has been fixed in the new version of the **openscap** package. As a result, OpenSCAP no longer fails during the evaluation of the STIG profile for RHEL 8 and other SCAP content that contains the **filehash58_test** OVAL test.

(BZ#1959570)

Ansible updates banner files only when needed

Previously, the playbook used for banner remediation always removed the file and recreated it. As a consequence, the banner file inodes were always modified regardless of need. With this update, the Ansible remediation playbook has been improved to use the **copy** module, which first compares existing content with the intended content and only updates the file when needed. As a result, banner files are only updated when the existing content differs from the intended content.

(BZ#1857179)

USB devices now work correctly with the DISA STIG profile

Previously, the DISA STIG profile enabled the **USBGuard** service but did not configure any initially connected USB devices. Consequently, the **USBGuard** service blocked any device that was not specifically allowed. This made some USB devices, such as smart cards, unreachable. With this update, the initial USBGuard configuration is generated when applying the DISA STIG profile and allows the use of any connected USB device. As a result, USB devices are not blocked and work correctly.

(BZ#1946252)

OSCAP Anaconda Addon now installs all selected packages in text mode

Previously, the **OSCAP Anaconda Addon** plugin did not evaluate rules that required certain partition layout or package installations and removals before the installation started when running in text mode. Consequently, when a security policy profile was specified using Kickstart and the installation was running in text mode, any additional packages required by a selected security profile were not installed. **OSCAP Anaconda Addon** now performs the required checks before the installation starts regardless of whether the installation is graphical or text-based, and all selected packages are installed also in text mode.

(BZ#1674001)

rpm_verify_permissions removed from the CIS profile

The **rpm_verify_permissions** rule, which compares file permissions to package default permissions, has been removed from the Center for Internet Security (CIS) Red Hat Enterprise Linux 8 Benchmark. With this update, the CIS profile is aligned with the CIS RHEL 8 benchmark, and as a result, this rule no longer affects users who harden their systems according to CIS.

(BZ#1843913)

leftikeport and rightikeport options work correctly

Previously, Libreswan ignored the **leftikeport** and **rightikeport** options in any host-to-host Libreswan connections. As a consequence, Libreswam used the default ports regardless of any non-default options settings. With this update, the issue is now fixed and you can use **leftikeport** and **rightikeport** connection options over the default options.

(BZ#1934058)

5.5. KERNEL

Certain BCC utilities do not display the "macro redefined" warning anymore

Macro redefinitions in some compiler-specific kernel headers caused some BPF Compiler Collection (BCC) utilities to display the following zero-impact warning:

```
warning: '__no_sanitize_address' macro redefined [-Wmacro-redefined]
```

With this update, the problem has been fixed by removing the macro redefinitions. As a result, the relevant BCC utilities no longer display the warning in this scenario.

(BZ#1907271)

kdump no longer fails to dump vmcore on SSH or NFS targets

Previously, when configuring a network interface card (NIC) port to a static IP address and setting **kdump** to dump **vmcore** on SSH or NFS dump targets, the **kdump** service started with the following error message:

```
ipcalc: command not found
```

Consequently, a **kdump** on SSH or NFS dump targets eventually failed.

This update fixes the problem and the **kexec-tools** utility no longer depends on the **ipcalc** tool for IP address and netmask calculation. As a result, the **kdump** works as expected when you use SSH or NFS dump targets.

(BZ#1931266)

Certain networking kernel drivers now properly display their version

The behavior for module versioning of many networking kernel drivers changed in RHEL 8.4. Consequently, those drivers did not display their version. Alternatively, after executing the **ethtool -i** command, the drivers displayed the **kernel** version instead of the **driver** version. This update fixes the bug by providing the kernel module strings. As a result, users can determine versions of the affected kernel drivers.

(BZ#1944639)

The **hwloc** commands now return correct data on single CPU Power9 and Power10 logical partitions

With the **hwloc** utility of version 2.2.0, any single-node Non-Uniform Memory Access (NUMA) system that ran a Power9 or Power10 CPU was considered to be "disallowed". Consequently, all **hwloc** commands did not work, because NODE0 (socket 0, CPU 0) was offline and the **hwloc** source code expected NODE0 to be online. The following error message was displayed:

```
Topology does not contain any NUMA node, aborting!
```

With this update, **hwloc** has been fixed so that its source code checks to see if NODE0 is online before querying it. If NODE0 is not online, the code proceeds to the next online NODE.

As a result, the **hwloc** command does not return any errors in the described scenario.

(BZ#1917560)

5.6. HIGH AVAILABILITY AND CLUSTERS

The **ocf:heartbeat:pgsql** resource agent and some third-party agents no longer fail to stop during a shutdown process

In the RHEL 8.4 GA release, Pacemaker's **crm_mon** command-line tool was modified to display a "shutting down" message rather than the usual cluster information when Pacemaker starts to shut down. As a consequence, shutdown progress, such as the stopping of resources, could not be monitored. In this situation, resource agents that parse **crm_mon** output in their stop operation (such as the **ocf:heartbeat:pgsql** agent distributed with the resource-agents package, or some custom or third-party agents) could fail to stop, leading to cluster problems. This bug has been fixed, and the described problem no longer occurs.

(BZ#1948620)

5.7. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS

pyodbc works again with **MariaDB 10.3**

The **pyodbc** module did not work with the **MariaDB 10.3** server included in the RHEL 8.4 release. The root cause in the **mariadb-connector-odbc** package has been fixed, and **pyodbc** now works with **MariaDB 10.3** as expected.

Note that earlier versions of the **MariaDB 10.3** server and the **MariaDB 10.5** server were not affected by this problem.

(BZ#1944692)

5.8. COMPILERS AND DEVELOPMENT TOOLS

GCC Toolset 11: GCC 11 now defaults to DWARF 4

While upstream GCC 11 defaults to using the DWARF 5 debugging format, GCC of GCC Toolset 11 defaults to DWARF 4 to stay compatible with RHEL 8 components, for example, **rpmbuild**.

(BZ#1974402)

The tunables framework now parses GLIBC_TUNABLES correctly

Previously, the tunables framework did not parse the **GLIBC_TUNABLES** environment variable correctly for non-setuid children of setuid programs. As a consequence, in some cases all tunables remained in non-setuid children of setuid programs. With this update, tunables in the **GLIBC_TUNABLES** environment variable are correctly parsed. As a result, only a restricted subset of identified tunables are now inherited by non-setuid children of setuid programs.

(BZ#1934155)

The semctl system call wrapper in glibc now treats SEM_STAT_ANY like SEM_STAT

Previously, the **semctl** system call wrapper in **glibc** did not treat the kernel argument **SEM_STAT_ANY** like **SEM_STAT**. As a result, **glibc** did not pass the address of the result object **struct semid_ds** to the kernel, so that the kernel failed to update it. With this update, **glibc** now treats **SEM_STAT_ANY** like **SEM_STAT**`, and as a result, applications can obtain **struct semid_ds** data using **SEM_STAT_ANY**.

(BZ#1912670)

Glibc now includes definitions for IPPROTO_ETHERNET, IPPROTO_MPTCP, and INADDR_ALLSNOOPERS_GROUP

Previously, the **Glibc** system library headers (**/usr/include/netinet/in.h**) did not include definitions of **IPPROTO_ETHERNET**, **IPPROTO_MPTCP**, and **INADDR_ALLSNOOPERS_GROUP**. As a consequence, applications needing these definitions failed to compile. With this update, the system library headers now include the new network constant definitions for **IPPROTO_ETHERNET**, **IPPROTO_MPTCP**, and **INADDR_ALLSNOOPERS_GROUP** resulting in correctly compiling applications.

(BZ#1930302)

gcc rebased to version 8.5

The GNU Compiler Collection (GCC) has been rebased to upstream version 8.5, which provides a number of bug fixes over the previous version.

(BZ#1946758)

Incorrect file decryption using OpenSSL aes-cbc mode

The OpenSSL EVP **aes-cbc** mode did not decrypt files correctly, because it expects to handle padding while the Go CryptoBlocks interface expects full blocks. This issue has been fixed by disabling padding before executing EVP operations in OpenSSL.

(BZ#1979100)

Using CryptBlocks multiple times over the same input stream leads to incorrect encryption

When Go FIPS mode is enabled, AES CBC CryptBlocks incorrectly re-initializes the initialization vector. As a result, using CryptBlocks multiple times over the input stream encrypts files incorrectly. To work around this issue, do not reinitialize IV in the **aes-cbc** interface. This action allows files to be encrypted correctly.

(BZ#1972825)

5.9. IDENTITY MANAGEMENT

FreeRADIUS no longer incorrectly generating default certificates when the bootstrap script is run

A bootstrap script runs each time FreeRADIUS is started. Previously, this script generated new testing certificates in the **/etc/raddb/certs** directory and as a result, the FreeRADIUS server sometimes failed to start as these testing certificates were invalid. For example, the certificates might have expired. With this update, the bootstrap script checks the **/etc/raddb/certs** directory and if it contains any testing or customer certificates, the script is not run and the FreeRADIUS server should start correctly.

Note that the testing certificates are only for testing purposes during the configuration of FreeRADIUS and should not be used in a real environment. The bootstrap script should be deleted once the users' certificates are used.

(BZ#1954521)

SSSD correctly evaluates the default setting for the Kerberos keytab name in /etc/krb5.conf

Previously, if you defined a non-standard location for your **krb5.keytab** file, SSSD did not use this location and used the default **/etc/krb5.keytab** location instead. As a result, when you tried to log into the system, the login failed as the **/etc/krb5.keytab** contained no entries.

With this update, SSSD now evaluates the **default_keytab_name** variable in the **/etc/krb5.conf** and uses the location specified by this variable. SSSD only uses the default **/etc/krb5.keytab** location if the **default_keytab_name** variable is not set.

(BZ#1737489)

Running sudo commands no longer exports the KRB5CCNAME environment variable

Previously, after running **sudo** commands, the environment variable **KRB5CCNAME** pointed to the Kerberos credential cache of the original user, which might not be accessible to the target user. As a result Kerberos related operations might fail as this cache is not accessible. With this update, running **sudo** commands no longer sets the **KRB5CCNAME** environment variable and the target user can use their default Kerberos credential cache.

(BZ#1879869)

Kerberos now only requests permitted encryption types

Previously, RHEL did not apply permitted encryption types specified in the **permitted_enctypes** parameter in the **/etc/krb5.conf** file if the **default_tgs_enctypes** or **default_tkt_enctypes** parameters were not set. Consequently, Kerberos clients were able to request deprecated cipher suites, such as RC4, which might cause other processes to fail. With this update, RHEL applies the encryption types set in **permitted_enctypes** to the default encryption types as well, and processes can only request permitted encryption types.

If you use Red Hat Identity Management (IdM) and want to set up a trust with Active Directory (AD), note that the RC4 cipher suite, which is deprecated in RHEL 8, is the default encryption type for users, services, and trusts between AD domains in an AD forest. You can use one of the following options:

- (Preferred): Enable strong AES encryption types in AD. For details, see the AD DS: Security: Kerberos "Unsupported etype" error when accessing a resource in a trusted domain Microsoft article.

- Use the **update-crypto-policies --set DEFAULT:AD-SUPPORT** command on RHEL hosts that should be members of an AD domain to enable the deprecated RC4 encryption type for backwards compatibility with AD.

(BZ#2005277)

▌Changelog cache can upload updates from a wrong starting point (CSN) | mmuehlfe@redhat.com

TODO https://bugzilla.redhat.com/show_bug.cgi?id=1898541

▌Internal unindexed searches in syncrepl | mmuehlfe@redhat.com

TODO https://bugzilla.redhat.com/show_bug.cgi?id=1951020

▌Internal unindexed searches in syncrepl | mmuehlfe@redhat.com

TODO https://bugzilla.redhat.com/show_bug.cgi?id=1951020

▌Internal unindexed searches in syncrepl | mmuehlfe@redhat.com

TODO https://bugzilla.redhat.com/show_bug.cgi?id=1951020

▌Internal unindexed searches in syncrepl | mmuehlfe@redhat.com

TODO https://bugzilla.redhat.com/show_bug.cgi?id=1951020

5.10. RED HAT ENTERPRISE LINUX SYSTEM ROLES

Role tasks no longer change when running the same output

Previously, several of the role tasks would report as **CHANGED** when running the same input once again, even if there were no changes. Consequently, the role was not acting idempotent. To fix the issue, perform the following actions:

- Check if configuration variables change before applying them. You can use the option **--check** for this verification.
- Do not add a **Last Modified: $date** header to the configuration file.

As a result, the role tasks are idempotent.

(BZ#1960375)

relayhost parameter no longer incorrectly defined in the Postfix documentation

Previously, the **relayhost** parameter of the Postfix RHEL System Role was defined as **relay_host** in the **doc /usr/share/doc/rhel-system-roles/postfix/README.md** documentation provided by **rhel-system-roles**. This update fixes the issue and the **relayhost** parameter is now correctly defined in the **Postfix** documentation.

(BZ#1866544)

Postfix RHEL System Role README.md no longer missing variables under the "Role Variables" section

Previously, the **Postfix** RHEL system role variables, such as **postfix_check**, **postfix_backup**, **postfix_backup_multiple** were not available under the "Role Variables" section. Consequently, users were not able to consult the Postfix role documentation. This update adds role variable documentation to the **Postfix** README section. The role variables are documented and available for users in the **doc/usr/share/doc/rhel-system-roles/postfix/README.md** documentation provided by **rhel-system-roles**.

(BZ#1961858)

Postfix role README no longer uses plain role name

Previously, the examples provided in the **/usr/share/ansible/roles/rhel-system-roles.postfix/README.md** used the plain version of the role name, **postfix**, instead of using **rhel-system-roles.postfix**. Consequently, users would consult the documentation and incorrectly use the plain role name instead of Full Qualified Role Name (FQRN). This update fixes the issue, and the documentation contains examples with the FQRN, **rhel-system-roles.postfix**, enabling users to correctly write playbooks.

(BZ#1958963)

The output log of timesync only reports harmful errors

Previously, the **timesync** RHEL System Role used the **ignore_errors** directive with separate checking for task failure in many tasks. Consequently, the output log of the successful role run was full of harmless errors. The users were safe to ignore those errors, but still they were distressing to see. In this update, the relevant tasks have been rewritten not to use **ignore_errors**. As a result, the output log is now clean, and only role-stopping errors are reported.

(BZ#1938014)

The requirements.txt file no longer missing in the Ansible collection

Previously, the **requirements.txt** file, responsible for specifying the python dependencies, was missing in the Ansible collection. This fix adds the missing file with the correct dependencies at the **/usr/share/ansible/collections/ansible_collections/redhat/rhel_system_roles/requirements.tx** path.

(BZ#1954747)

Traceback no longer observed when set type: partition for storage_pools

Previously, when setting the variable **type** as **partition** for **storage_pools** in a playbook, running this playbook would fail and indicate **traceback**. This update fixes the issue and the **Traceback** error no longer appears.

(BZ#1854187)

SElinux role no longer perform unnecessary reloads

Previously, the **SElinux** role would not check if changes were actually applied before reloading the **SElinux** policy. As a consequence, the **SElinux** policy was being reloaded unnecessarily, which had an impact on the system resources. With this fix, the **SElinux** role now uses ansible handlers and conditionals to ensure that the policy is only reloaded if there is a change. As a result, the **SElinux** role runs much faster.

(BZ#1757869)

5.11. RHEL IN CLOUD ENVIRONMENTS

nm-cloud-setup utility now sets the correct default route on Microsoft Azure

Previously, on Microsoft Azure, the **nm-cloud-setup** utility failed to detect the correct gateway of the cloud environment. As a consequence, the utility set an incorrect default route, and connectivity failed. This update fixes the problem. As a result, **nm-cloud-setup** utility now sets the correct default route on Microsoft Azure.

(BZ#1912236)

SSH keys are now generated correctly on EC2 instances created from a backup AMI

Previously, when creating a new Amazon EC2 instance of RHEL 8 from a backup Amazon Machine Image (AMI), **cloud-init** deleted existing SSH keys on the VM but did not create new ones. Consequently, the VM in some cases could not connect to the host.

This problem has been fixed for newly created RHEL 8.5 VMs. For VMs that were upgraded from RHEL 8.4 or earlier, you must work around the issue manually.

To do so, edit the **cloud.cfg** file and changing the **ssh_genkeytypes:** ~ line to **ssh_genkeytypes: ['rsa', 'ecdsa', 'ed25519']**. This makes it possible for SSH keys to be deleted and generated correctly when provisioning a RHEL 8 VM in the described circumstances.

(BZ#1957532)

RHEL 8 running on AWS ARM64 instances can now reach the specified network speed

When using RHEL 8 as a guest operating system in a virtual machine (VM) that runs on an Amazon Web Services (AWS) ARM64 instance, the VM previously had lower than expected network performance when the **iommu.strict=1** kernel parameter was used or when no **iommu.strict** parameter was defined.

This problem no longer occurs in RHEL 8.5 Amazon Machine Images (AMIs) provided by Red Hat. In other types of images, you can work around the issue by changing the parameter to **iommu.strict=0**. This includes:

- RHEL 8.4 and earlier images
- RHEL 8.5 images upgraded from an earlier version using **yum update**
- RHEL 8.5 images not provided by Red Hat

(BZ#1836058)

Core dumping RHEL 8 virtual machines with certain NICs to a remote machine on Azure no longer takes an excessive amount of time

Previously, using the **kdump** utility to save the core dump file of a RHEL 8 virtual machine (VM) on a Microsoft Azure hypervisor to a remote machine did not work correctly when the VM was using a NIC with enabled accelerated networking. As a consequence, the dump file was saved after approximately 200 seconds, instead of immediately. In addition, the following error message was logged on the console before the dump file is saved.

```
device (eth0): linklocal6: DAD failed for an EUI-64 address
```

With this update, the underlying code has been fixed, and in the described circumstances, dump files are now saved immediately.

(BZ#1854037)

CHAPTER 6. TECHNOLOGY PREVIEWS

This part provides a list of all Technology Previews available in Red Hat Enterprise Linux 8.5 Beta.

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

6.1. INSTALLER AND IMAGE CREATION

Red Hat Connector available as a Technology Preview

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

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

(BZ#1957316)

6.2. SHELLS AND COMMAND-LINE TOOLS

IBM Z architecture in ReaR available as a Technology Preview

The basic support for IBM Z architecture was added to Relax and Recover (ReaR) and is now available as a Technology Preview. ReaR on IBM Z architecture is currently supported only in the z/VM environment. The support for backing up and recovering logical partitions (LPARs) has not been tested.

The only output method currently supported is Initial Program Load (IPL). IPL produces a kernel and an initial ramdisk (initrd) that can be used with the **zIPL** bootloader.

For further information read the Using ReaR rescue image on IBM System Z architecture .

(BZ#1868421)

6.3. NETWORKING

KTLS available as a Technology Preview

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

(BZ#1570255)

AF_XDP available as a Technology Preview

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

(BZ#1633143)

XDP features that are available as Technology Preview

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

- Loading XDP programs on architectures other than AMD and Intel 64-bit. Note that the **libxdp** library is not available for architectures other than AMD and Intel 64-bit.
- The XDP hardware offloading. Before using this feature, see Unloading XDP programs fails on Netronome network cards that use the nfp driver.

(BZ#1889737)

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

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

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

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

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

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

(BZ#1814836, BZ#1856415)

act_mpls module available as a Technology Preview

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

(BZ#1839311)

Improved Multipath TCP support is available as a Technology Preview

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

RHEL 8.4 offers additional features, such as:

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

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

For further details see, Getting started with Multipath TCP.

(JIRA:RHELPLAN-57712)

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

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

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

(BZ#1906489)

The nispor package is now available as a Technology Preview

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

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

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

  ```
  # yum install nispor
  ```

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

  ```
  # yum install nmstate
  ```

  nispor is listed as the dependency.

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

(BZ#1848817)

6.4. KERNEL

The kexec fast reboot feature is available as Technology Preview

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

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

(BZ#1769727)

The accel-config package available as a Technology Preview

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

(BZ#1843266)

SGX available as a Technology Preview

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

(BZ#1660337)

eBPF available as a Technology Preview

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

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

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

There are numerous components shipped by Red Hat that utilize the **eBPF** virtual machine. Each component is in a different development phase, and thus not all components are currently fully supported. All components are available as a Technology Preview, unless a specific component is indicated as supported.

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

- **bpftrace**, a high-level tracing language that utilizes the **eBPF** virtual machine.
- **AF_XDP**, a socket for connecting the **eXpress Data Path (XDP)**path to user space for applications that prioritize packet processing performance.

(BZ#1559616)

The data streaming accelerator driver for kernel is available as a Technology Preview

The data streaming accelerator (DSA) driver for the kernel is currently available as a Technology Preview. DSA is an Intel CPU integrated accelerator and supports a shared work queue with process address space ID (pasid) submission and shared virtual memory (SVM).

(BZ#1837187)

The stmmac driver is available as a Technology Preview

Red Hat provides the usage of **stmmac** for Intel® Elkhart Lake systems on a chip (SoCs) as an unsupported Technology Preview.

(BZ#1905243)

6.5. FILE SYSTEMS AND STORAGE

NVMe/TCP is available as a Technology Preview

Accessing and sharing Nonvolatile Memory Express (NVMe) storage over TCP/IP networks (NVMe/TCP) and its corresponding **nvme-tcp.ko** and **nvmet-tcp.ko** kernel modules have been added as a Technology Preview.

The use of NVMe/TCP as either a storage client or a target is manageable with tools provided by the **nvme-cli** and **nvmetcli** packages.

The NVMe/TCP target Technology Preview is included only for testing purposes and is not currently planned for full support.

(BZ#1696451)

File system DAX is now available for ext4 and XFS as a Technology Preview

In Red Hat Enterprise Linux 8, file system DAX is available as a Technology Preview. DAX provides a means for an application to directly map persistent memory into its address space. To use DAX, a system must have some form of persistent memory available, usually in the form of one or more Non-Volatile Dual In-line Memory Modules (NVDIMMs), and a file system that supports DAX must be created on the NVDIMM(s). Also, the file system must be mounted with the **dax** mount option. Then, an **mmap** of a file on the dax-mounted file system results in a direct mapping of storage into the application's address space.

(BZ#1627455)

OverlayFS

OverlayFS is a type of union file system. It enables you to overlay one file system on top of another. Changes are recorded in the upper file system, while the lower file system remains unmodified. This allows multiple users to share a file-system image, such as a container or a DVD-ROM, where the base image is on read-only media.

OverlayFS remains a Technology Preview under most circumstances. As such, the kernel logs warnings when this technology is activated.

Full support is available for OverlayFS when used with supported container engines (**podman**, **cri-o**, or **buildah**) under the following restrictions:

- OverlayFS is supported for use only as a container engine graph driver. Its use is supported only for container COW content, not for persistent storage. You must place any persistent storage on non-OverlayFS volumes. You can use only the default container engine configuration: one level of overlay, one lowerdir, and both lower and upper levels are on the same file system.

- Only XFS is currently supported for use as a lower layer file system.

Additionally, the following rules and limitations apply to using OverlayFS:

- The OverlayFS kernel ABI and user-space behavior are not considered stable, and might change in future updates.
- OverlayFS provides a restricted set of the POSIX standards. Test your application thoroughly before deploying it with OverlayFS. The following cases are not POSIX-compliant:
    - Lower files opened with **O_RDONLY** do not receive **st_atime** updates when the files are read.
    - Lower files opened with **O_RDONLY**, then mapped with **MAP_SHARED** are inconsistent with subsequent modification.
    - Fully compliant **st_ino** or **d_ino** values are not enabled by default on RHEL 8, but you can enable full POSIX compliance for them with a module option or mount option.
      To get consistent inode numbering, use the **xino=on** mount option.

      You can also use the **redirect_dir=on** and **index=on** options to improve POSIX compliance. These two options make the format of the upper layer incompatible with an overlay without these options. That is, you might get unexpected results or errors if you create an overlay with **redirect_dir=on** or **index=on**, unmount the overlay, then mount the overlay without these options.
- To determine whether an existing XFS file system is eligible for use as an overlay, use the following command and see if the **ftype=1** option is enabled:

  ```
  # xfs_info /mount-point | grep ftype
  ```
- SELinux security labels are enabled by default in all supported container engines with OverlayFS.
- Several known issues are associated with OverlayFS in this release. For details, see *Non-standard behavior* in the Linux kernel documentation: https://www.kernel.org/doc/Documentation/filesystems/overlayfs.txt.

For more information about OverlayFS, see the Linux kernel documentation: https://www.kernel.org/doc/Documentation/filesystems/overlayfs.txt.

(BZ#1690207)

Stratis is now available as a Technology Preview

Stratis is a new local storage manager. It provides managed file systems on top of pools of storage with additional features to the user.

Stratis enables you to more easily perform storage tasks such as:

- Manage snapshots and thin provisioning
- Automatically grow file system sizes as needed

- Maintain file systems

To administer Stratis storage, use the **stratis** utility, which communicates with the **stratisd** background service.

Stratis is provided as a Technology Preview.

For more information, see the Stratis documentation: Managing layered local storage with Stratis.

RHEL 8.3 updated Stratis to version 2.1.0. For more information, see Stratis 2.1.0 Release Notes.

(JIRA:RHELPLAN-1212)

Setting up a Samba server on an IdM domain member is provided as a Technology Preview

With this update, you can now set up a Samba server on an Identity Management (IdM) domain member. The new **ipa-client-samba** utility provided by the same-named package adds a Samba-specific Kerberos service principal to IdM and prepares the IdM client. For example, the utility creates the **/etc/samba/smb.conf** with the ID mapping configuration for the **sss** ID mapping back end. As a result, administrators can now set up Samba on an IdM domain member.

Due to IdM Trust Controllers not supporting the Global Catalog Service, AD-enrolled Windows hosts cannot find IdM users and groups in Windows. Additionally, IdM Trust Controllers do not support resolving IdM groups using the Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) protocols. As a consequence, AD users can only access the Samba shares and printers from IdM clients.

For details, see Setting up Samba on an IdM domain member.

(JIRA:RHELPLAN-13195)

6.6. HIGH AVAILABILITY AND CLUSTERS

Pacemaker **podman** bundles available as a Technology Preview

Pacemaker container bundles now run on Podman, with the container bundle feature being available as a Technology Preview. There is one exception to this feature being Technology Preview: Red Hat fully supports the use of Pacemaker bundles for Red Hat Openstack.

(BZ#1619620)

Heuristics in **corosync-qdevice** available as a Technology Preview

Heuristics are a set of commands executed locally on startup, cluster membership change, successful connect to **corosync-qnetd**, and, optionally, on a periodic basis. When all commands finish successfully on time (their return error code is zero), heuristics have passed; otherwise, they have failed. The heuristics result is sent to **corosync-qnetd** where it is used in calculations to determine which partition should be quorate.

(BZ#1784200)

New **fence-agents-heuristics-ping** fence agent

As a Technology Preview, Pacemaker now supports the **fence_heuristics_ping** agent. This agent aims to open a class of experimental fence agents that do no actual fencing by themselves but instead exploit the behavior of fencing levels in a new way.

If the heuristics agent is configured on the same fencing level as the fence agent that does the actual fencing but is configured before that agent in sequence, fencing issues an **off** action on the heuristics agent before it attempts to do so on the agent that does the fencing. If the heuristics agent gives a negative result for the **off** action it is already clear that the fencing level is not going to succeed, causing Pacemaker fencing to skip the step of issuing the **off** action on the agent that does the fencing. A heuristics agent can exploit this behavior to prevent the agent that does the actual fencing from fencing a node under certain conditions.

A user might want to use this agent, especially in a two-node cluster, when it would not make sense for a node to fence the peer if it can know beforehand that it would not be able to take over the services properly. For example, it might not make sense for a node to take over services if it has problems reaching the networking uplink, making the services unreachable to clients, a situation which a ping to a router might detect in that case.

(BZ#1775847)

Automatic removal of location constraint following resource move available as a Technology Preview

When you execute the **pcs resource move** command, this adds a constraint to the resource to prevent it from running on the node on which it is currently running. A new **--autodelete** option for the **pcs resource move** command is now available as a Technology Preview. When you specify this option, the location constraint that the command creates is automatically removed once the resource has been moved.

(BZ#1847102)

6.7. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS

A new **nodejs:16** module stream available as a Technology Preview

A new module stream, **nodejs:16**, is now available as a Technology Preview. A future update will provide a Long Term Support (LTS) version of **Node.js 16**, which will be fully supported.

Node.js 16 included in RHEL 8.5 provides numerous new features and bug and security fixes over **Node.js 14** distributed in RHEL 8.3.

Notable changes include:

- The **V8** engine has been upgraded to version 9.2.
- The **npm** package manager has been upgraded to version 7.21.0.
- A new **Timers Promises** API provides an alternative set of timer functions that return **Promise** objects.
- **Node.js** now provides a new experimental **Web Streams** API.

To install the **nodejs:16** module stream, use:

```
# yum module install nodejs:16
```

If you want to upgrade from the **nodejs:14** stream, see Switching to a later stream .

(BZ#1953991)

6.8. IDENTITY MANAGEMENT

Identity Management JSON-RPC API available as Technology Preview

An API is available for Identity Management (IdM). To view the API, IdM also provides an API browser as a Technology Preview.

Previously, the IdM API was enhanced to enable multiple versions of API commands. These enhancements could change the behavior of a command in an incompatible way. Users are now able to continue using existing tools and scripts even if the IdM API changes. This enables:

- Administrators to use previous or later versions of IdM on the server than on the managing client.
- Developers can use a specific version of an IdM call, even if the IdM version changes on the server.

In all cases, the communication with the server is possible, regardless if one side uses, for example, a newer version that introduces new options for a feature.

For details on using the API, see Using the Identity Management API to Communicate with the IdM Server (TECHNOLOGY PREVIEW).

(BZ#1664719)

DNSSEC available as Technology Preview in IdM

Identity Management (IdM) servers with integrated DNS now support DNS Security Extensions (DNSSEC), a set of extensions to DNS that enhance security of the DNS protocol. DNS zones hosted on IdM servers can be automatically signed using DNSSEC. The cryptographic keys are automatically generated and rotated.

Users who decide to secure their DNS zones with DNSSEC are advised to read and follow these documents:

- DNSSEC Operational Practices, Version 2: http://tools.ietf.org/html/rfc6781#section-2
- Secure Domain Name System (DNS) Deployment Guide: http://dx.doi.org/10.6028/NIST.SP.800-81-2
- DNSSEC Key Rollover Timing Considerations: http://tools.ietf.org/html/rfc7583

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

(BZ#1664718)

ACME available as a Technology Preview

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

In RHEL, the ACME service uses the Red Hat Certificate System (RHCS) PKI ACME responder. The RHCS ACME subsystem is automatically deployed on every certificate authority (CA) server in the IdM deployment, but it does not service requests until the administrator enables it. RHCS uses the

acmeIPAServerCert profile when issuing ACME certificates. The validity period of issued certificates is 90 days. Enabling or disabling the ACME service affects the entire IdM deployment.

IMPORTANT

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

WARNING

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

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

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

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

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

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

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

(JIRA:RHELPLAN-58596)

6.9. DESKTOP

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

The GNOME desktop environment is now available for the 64-bit ARM architecture as a Technology Preview. This enables administrators to configure and manage servers from a graphical user interface (GUI) remotely, using the VNC session.

As a consequence, new administration applications are available on the 64-bit ARM architecture. For example: **Disk Usage Analyzer** (**baobab**), **Firewall Configuration** (**firewall-config**), **Red Hat Subscription Manager** (**subscription-manager**), or the **Firefox** web browser. Using **Firefox**, administrators can connect to the local Cockpit daemon remotely.

(JIRA:RHELPLAN-27394, BZ#1667225, BZ#1667516, BZ#1724302)

GNOME desktop on IBM Z is available as a Technology Preview

The GNOME desktop, including the Firefox web browser, is now available as a Technology Preview on the IBM Z architecture. You can now connect to a remote graphical session running GNOME using VNC to configure and manage your IBM Z servers.

(JIRA:RHELPLAN-27737)

6.10. GRAPHICS INFRASTRUCTURES

VNC remote console available as a Technology Preview for the 64-bit ARM architecture

On the 64-bit ARM architecture, the Virtual Network Computing (VNC) remote console is available as a Technology Preview. Note that the rest of the graphics stack is currently unverified for the 64-bit ARM architecture.

(BZ#1698565)

6.11. RED HAT ENTERPRISE LINUX SYSTEM ROLES

HA Cluster RHEL System Role available as a Technology Preview

The High Availability Cluster (HA Cluster) role is now available as a Technology Preview. Currently, the following notable configurations are available:

- Configuring nodes, fence device, resources, resource groups, and resource clones including meta attributes and resource operations
- Configuring cluster properties
- Configuring multi-link clusters
- Configuring custom cluster names and node names
- Configuring whether clusters start automatically on boot

The HA system role does not currently support constraints. Running the role after constraints are configured manually will remove the constraints, as well as any configuration not supported by the role.

The HA system role does not currently support SBD.

(BZ#1893743, BZ#1982913)

6.12. VIRTUALIZATION

KVM virtualization is usable in RHEL 8 Hyper-V virtual machines

As a Technology Preview, nested KVM virtualization can now be used on the Microsoft Hyper-V hypervisor. As a result, you can create virtual machines on a RHEL 8 guest system running on a Hyper-V host.

Note that currently, this feature only works on Intel and AMD systems. In addition, nested virtualization is in some cases not enabled by default on Hyper-V. To enable it, see the following Microsoft documentation:

https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/user-guide/nested-virtualization

(BZ#1519039)

AMD SEV for KVM virtual machines

As a Technology Preview, RHEL 8 provides the Secure Encrypted Virtualization (SEV) feature for AMD EPYC host machines that use the KVM hypervisor. If enabled on a virtual machine (VM), SEV encrypts VM memory so that the host cannot access data on the VM. This increases the security of the VM if the host is successfully infected by malware.

Note that the number of VMs that can use this feature at a time on a single host is determined by the host hardware. Current AMD EPYC processors support up to 509 running VMs using SEV.

Also note that for VMs with SEV configured to be able to boot, you must also configure the VM with a hard memory limit. To do so, add the following to the VM's XML configuration:

```
<memtune>
<hard_limit unit='KiB'>N</hard_limit>
</memtune>
```

The recommended value for N is equal to or greater then the guest RAM + 256 MiB. For example, if the guest is assigned 2 GiB RAM, N should be 2359296 or greater.

(BZ#1501618, BZ#1501607, JIRA:RHELPLAN-7677)

Intel vGPU

As a Technology Preview, it is now possible to divide a physical Intel GPU device into multiple virtual devices referred to as **mediated devices**. These mediated devices can then be assigned to multiple virtual machines (VMs) as virtual GPUs. As a result, these VMs share the performance of a single physical Intel GPU.

Note that only selected Intel GPUs are compatible with the vGPU feature.

In addition, it is possible to enable a VNC console operated by Intel vGPU. By enabling it, users can connect to a VNC console of the VM and see the VM's desktop hosted by Intel vGPU. However, this currently only works for RHEL guest operating systems.

(BZ#1528684)

Creating nested virtual machines

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

(JIRA:RHELPLAN-14047, JIRA:RHELPLAN-24437)

Select Intel network adapters now support SR-IOV in RHEL guests on Hyper-V

As a Technology Preview, Red Hat Enterprise Linux guest operating systems running on a Hyper-V hypervisor can now use the single-root I/O virtualization (SR-IOV) feature for Intel network adapters supported by the **ixgbevf** and **iavf** drivers. This feature is enabled when the following conditions are met:

- SR-IOV support is enabled for the network interface controller (NIC)
- SR-IOV support is enabled for the virtual NIC
- SR-IOV support is enabled for the virtual switch
- The virtual function (VF) from the NIC is attached to the virtual machine

The feature is currently supported with Microsoft Windows Server 2019 and 2016.

(BZ#1348508)

ESXi hypervisor and SEV-ES available as a Technology Preview for RHEL VMs

As a Technology Preview, in RHEL 8.4 and later, you can enable the AMD Secure Encrypted Virtualization-Encrypted State (SEV-ES) to secure RHEL virtual machines (VMs) on VMware's ESXi hypervisor, versions 7.0.2 and later.

(BZ#1904496)

Sharing files between hosts and VMs using virtiofs

As a Technology Preview, RHEL 8 now provides the virtio file system (**virtiofs**). Using **virtiofs**, you can efficiently share files between your host system and its virtual machines (VM).

(BZ#1741615)

6.13. CONTAINERS

The crun is available as a Technology Preview

The **crun** OCI runtime is now available for the **container-tools:rhel8** module as a Technology Preview. The **crun** container runtime supports an annotation that allows the container to access the rootless user's additional groups. This is useful for volume mounting in a directory where setgid is set, or where the user only has group access. Currently, neither the **crun** or **runc** runtimes fully support **cgroupsv2**.

(BZ#1841438)

A podman container image is available as a Technology Preview

The **registry.redhat.io/rhel8/podman** container image is a containerized implementation of the **podman** package. The **podman** tool is used for managing containers and images, volumes mounted into those containers, and pods made of groups of containers.

(JIRA:RHELPLAN-56659)

CNI plugins are available in Podman as a Technology Preview

CNI plugins are now available to use in Podman rootless mode as a Technology Preview. To enable this feature, users are required to build their own rootless CNI infrastructure container image.

(BZ#1932083)

New ubi8/nodejs-16 and ubi8/nodejs-16-minimal container images available as a Technology Preview

The **ubi8/nodejs-16** and **ubi8/nodejs-16-minimal** container images are now available as a Technology Preview. The container images include **Node.js 16**.

A future update to these container images will provide a Long Term Support (LTS) version of **Node.js 16**, which will be fully supported.

(BZ#2001020)

CHAPTER 7. DEPRECATED FUNCTIONALITY

This part provides an overview of functionality that has been *deprecated* in Red Hat Enterprise Linux 8.

Deprecated functionality continues to be supported until the end of life of Red Hat Enterprise Linux 8. Deprecated functionality will likely not be supported in future major releases of this product and is not recommended for new deployments. For the most recent list of deprecated functionality within a particular major release, refer to the latest version of release documentation.

Deprecated hardware components are not recommended for new deployments on the current or future major releases. Hardware driver updates are limited to security and critical fixes only. Red Hat recommends replacing this hardware as soon as reasonably feasible.

A package can be deprecated and not recommended for further use. Under certain circumstances, a package can be removed from a product. Product documentation then identifies more recent packages that offer functionality similar, identical, or more advanced to the one deprecated, and provides further recommendations.

For information regarding functionality that is present in RHEL 7 but has been *removed* in RHEL 8, see Considerations in adopting RHEL 8 .

7.1. INSTALLER AND IMAGE CREATION

Several Kickstart commands and options have been deprecated

Using the following commands and options in RHEL 8 Kickstart files will print a warning in the logs.

- **auth** or **authconfig**
- **device**
- **deviceprobe**
- **dmraid**
- **install**
- **lilo**
- **lilocheck**
- **mouse**
- **multipath**
- **bootloader --upgrade**
- **ignoredisk --interactive**
- **partition --active**
- **reboot --kexec**

Where only specific options are listed, the base command and its other options are still available and not deprecated.

For more details and related changes in Kickstart, see the Kickstart changes section of the *Considerations in adopting RHEL 8* document.

(BZ#1642765)

The --interactive option of the **ignoredisk** Kickstart command has been deprecated

Using the **--interactive option** in future releases of Red Hat Enterprise Linux will result in a fatal installation error. It is recommended that you modify your Kickstart file to remove the option.

(BZ#1637872)

The Kickstart **autostep** command has been deprecated

The **autostep** command has been deprecated. The related section about this command has been removed from the RHEL 8 documentation.

(BZ#1904251)

lorax-composer back end for Image Builder is deprecated in RHEL 8

The previous back end **lorax-composer** for Image Builder is considered deprecated. It will only receive select fixes for the rest of the Red Hat Enterprise Linux 8 life cycle and will be omitted from future major releases. Red Hat recommends that you uninstall **lorax-composer** the and install **osbuild-composer** back end instead.

See Composing a customized RHEL system image for more details.

(BZ#1893767)

7.2. SOFTWARE MANAGEMENT

rpmbuild --sign is deprecated

With this update, the **rpmbuild --sign** command has become deprecated. Using this command in future releases of Red Hat Enterprise Linux can result in an error. It is recommended that you use the **rpmsign** command instead.

(BZ#1688849)

7.3. SHELLS AND COMMAND-LINE TOOLS

The **OpenEXR** component has been deprecated

The **OpenEXR** component has been deprecated. Hence, the support for the **EXR** image format has been dropped from the **imagecodecs** module.

(BZ#1886310)

7.4. SECURITY

NSS SEED ciphers are deprecated

The Mozilla Network Security Services (**NSS**) library will not support TLS cipher suites that use a SEED cipher in a future release. To ensure smooth transition of deployments that rely on SEED ciphers when NSS removes support, Red Hat recommends enabling support for other cipher suites.

Note that SEED ciphers are already disabled by default in RHEL.

(BZ#1817533)

TLS 1.0 and TLS 1.1 are deprecated

The TLS 1.0 and TLS 1.1 protocols are disabled in the **DEFAULT** system-wide cryptographic policy level. If your scenario, for example, a video conferencing application in the Firefox web browser, requires using the deprecated protocols, switch the system-wide cryptographic policy to the **LEGACY** level:

```
# update-crypto-policies --set LEGACY
```

For more information, see the Strong crypto defaults in RHEL 8 and deprecation of weak crypto algorithms Knowledgebase article on the Red Hat Customer Portal and the **update-crypto-policies(8)** man page.

(BZ#1660839)

DSA is deprecated in RHEL 8

The Digital Signature Algorithm (DSA) is considered deprecated in Red Hat Enterprise Linux 8. Authentication mechanisms that depend on DSA keys do not work in the default configuration. Note that **OpenSSH** clients do not accept DSA host keys even in the **LEGACY** system-wide cryptographic policy level.

(BZ#1646541)

SSL2 Client Hello has been deprecated in NSS

The Transport Layer Security (**TLS**) protocol version 1.2 and earlier allow to start a negotiation with a **Client Hello** message formatted in a way that is backward compatible with the Secure Sockets Layer (**SSL**) protocol version 2. Support for this feature in the Network Security Services (**NSS**) library has been deprecated and it is disabled by default.

Applications that require support for this feature need to use the new **SSL_ENABLE_V2_COMPATIBLE_HELLO** API to enable it. Support for this feature may be removed completely in future releases of Red Hat Enterprise Linux 8.

(BZ#1645153)

TPM 1.2 is deprecated

The Trusted Platform Module (TPM) secure cryptoprocessor standard was updated to version 2.0 in 2016. TPM 2.0 provides many improvements over TPM 1.2, and it is not backward compatible with the previous version. TPM 1.2 is deprecated in RHEL 8, and it might be removed in the next major release.

(BZ#1657927)

crypto-policies derived properties are now deprecated

With the introduction of scopes for **crypto-policies** directives in custom policies, the following derived properties have been deprecated: **tls_cipher**, **ssh_cipher**, **ssh_group**, **ike_protocol**, and **sha1_in_dnssec**. Additionally, the use of the **protocol** property without specifying a scope is now deprecated as well. See the **crypto-policies(7)** man page for recommended replacements.

(BZ#2011208)

Runtime disabling SELinux using /etc/selinux/config is now deprecated

Runtime disabling SELinux using the **SELINUX=disabled** option in the **/etc/selinux/config** file has been deprecated. In RHEL 9, when you disable SELinux only through **/etc/selinux/config**, the system starts with SELinux enabled but with no policy loaded.

If your scenario really requires to completely disable SELinux, Red Hat recommends disabling SELinux by adding the **selinux=0** parameter to the kernel command line as described in the Changing SELinux modes at boot time section of the Using SELinux title.

(BZ#1932222)

The ipa SELinux module removed from selinux-policy

The **ipa** SELinux module has been removed from the **selinux-policy** package because it is no longer maintained. The functionality is now included in the **ipa-selinux** subpackage.

If your scenario requires the use of types or interfaces from the **ipa** module in a local SELinux policy, install the **ipa-selinux** package.

(BZ#1461914)

7.5. NETWORKING

Network scripts are deprecated in RHEL 8

Network scripts are deprecated in Red Hat Enterprise Linux 8 and they are no longer provided by default. The basic installation provides a new version of the **ifup** and **ifdown** scripts which call the **NetworkManager** service through the **nmcli** tool. In Red Hat Enterprise Linux 8, to run the **ifup** and the **ifdown** scripts, NetworkManager must be running.

Note that custom commands in **/sbin/ifup-local**, **ifdown-pre-local** and **ifdown-local** scripts are not executed.

If any of these scripts are required, the installation of the deprecated network scripts in the system is still possible with the following command:

```
~]# yum install network-scripts
```

The **ifup** and **ifdown** scripts link to the installed legacy network scripts.

Calling the legacy network scripts shows a warning about their deprecation.

(BZ#1647725)

The dropwatch tool is deprecated

The **dropwatch** tool has been deprecated. The tool will not be supported in future releases. Thus the tool is not recommended for new deployments. As a replacement of this package, Red Hat recommends to use the **perf** command line tool.

For more information on using the **perf** command line tool, see the Getting started with Perf section on the Red Hat customer portal or the **perf** man page.

(BZ#1929173)

The cgdcbxd package is deprecated

Control group data center bridging exchange daemon (**cgdcbxd**) is a service to monitor data center bridging (DCB) netlink events and manage the **net_prio control** group subsystem. Starting with RHEL 8.5, the **cgdcbxd** package is deprecated and will be removed in the next major RHEL release.

(BZ#2006665)

7.6. KERNEL

Kernel live patching now covers all RHEL minor releases

Since RHEL 8.1, kernel live patches have been provided for selected minor release streams of RHEL covered under the Extended Update Support (EUS) policy to remediate Critical and Important Common Vulnerabilities and Exposures (CVEs). To accommodate the maximum number of concurrently covered kernels and use cases, the support window for each live patch will be decreased from 12 to 6 months for every minor, major and zStream version of the kernel. It means that on the day a kernel live patch is released, it will cover every minor release and scheduled errata kernel delivered in the past 6 months. For example, 8.4.x will have a one-year support window, but 8.4.x+1 will have 6 months.

For more information about this feature, see Applying patches with kernel live patching .

For details about available kernel live patches, see Kernel Live Patch life cycles .

(BZ#1958250)

Installing RHEL for Real Time 8 using diskless boot is now deprecated

Diskless booting allows multiple systems to share a root file system via the network. While convenient, diskless boot is prone to introducing network latency in realtime workloads. With a future minor update of RHEL for Real Time 8, the diskless booting feature will no longer be supported.

(BZ#1748980)

7.7. FILE SYSTEMS AND STORAGE

LVM mirror is deprecated

The LVM **mirror** segment type is now deprecated. Support for **mirror** will be removed in a future major release of RHEL.

Red Hat recommends that you use LVM RAID 1 devices with a segment type of **raid1** instead of **mirror**. The **raid1** segment type is the default RAID configuration type and replaces **mirror** as the recommended solution.

To convert **mirror** devices to **raid1**, see Converting a mirrored LVM device to a RAID1 device .

LVM **mirror** has several known issues. For details, see known issues in file systems and storage .

(BZ#1827628)

peripety is deprecated

The **peripety** package is deprecated since RHEL 8.3.

The Peripety storage event notification daemon parses system storage logs into structured storage events. It helps you investigate storage issues.

(BZ#1871953)

VDO write modes other than async are deprecated

VDO supports several write modes in RHEL 8:

- **sync**
- **async**
- **async-unsafe**
- **auto**

Starting with RHEL 8.4, the following write modes are deprecated:

sync

Devices above the VDO layer cannot recognize if VDO is synchronous, and consequently, the devices cannot take advantage of the VDO **sync** mode.

async-unsafe

VDO added this write mode as a workaround for the reduced performance of **async** mode, which complies to Atomicity, Consistency, Isolation, and Durability (ACID). Red Hat does not recommend **async-unsafe** for most use cases and is not aware of any users who rely on it.

auto

This write mode only selects one of the other write modes. It is no longer necessary when VDO supports only a single write mode.

These write modes will be removed in a future major RHEL release.

The recommended VDO write mode is now **async**.

For more information on VDO write modes, see Selecting a VDO write mode.

(JIRA:RHELPLAN-70700)

NFSv3 over UDP has been disabled

The NFS server no longer opens or listens on a User Datagram Protocol (UDP) socket by default. This change affects only NFS version 3 because version 4 requires the Transmission Control Protocol (TCP).

NFS over UDP is no longer supported in RHEL 8.

(BZ#1592011)

VDO manager has been deprecated

The python-based VDO management software has been deprecated and will be removed from RHEL 9. In RHEL 9, it will be replaced by the LVM-VDO integration. It is, therefore, recommended to create VDO volumes using the **lvcreate** command.

The existing volumes created using the VDO management software can be converted using the **/usr/sbin/lvm_import_vdo** script, provided by the **lvm2** package. For more information on the LVM-VDO implementation, see Introduction to VDO on LVM.

(BZ#1949163)

The elevator kernel command line parameter is deprecated

The **elevator** kernel command line parameter was used in earlier RHEL releases to set the disk scheduler for all devices. In RHEL 8, the parameter is deprecated.

The upstream Linux kernel has removed support for the **elevator** parameter, but it is still available in RHEL 8 for compatibility reasons.

Note that the kernel selects a default disk scheduler based on the type of device. This is typically the optimal setting. If you require a different scheduler, Red Hat recommends that you use **udev** rules or the Tuned service to configure it. Match the selected devices and switch the scheduler only for those devices.

For more information, see Setting the disk scheduler.

(BZ#1665295)

7.8. HIGH AVAILABILITY AND CLUSTERS

pcs commands that support the clufter tool have been deprecated

The **pcs** commands that support the **clufter** tool for analyzing cluster configuration formats have been deprecated. These commands now print a warning that the command has been deprecated and sections related to these commands have been removed from the **pcs** help display and the **pcs(8)** man page.

The following commands have been deprecated:

- **pcs config import-cman** for importing CMAN / RHEL6 HA cluster configuration
- **pcs config export** for exporting cluster configuration to a list of **pcs** commands which recreate the same cluster

(BZ#1851335)

7.9. COMPILERS AND DEVELOPMENT TOOLS

libdwarf has been deprecated

The **libdwarf** library has been deprecated in RHEL 8. The library will likely not be supported in future major releases. Instead, use the **elfutils** and **libdw** libraries for applications that wish to process ELF/DWARF files.

Alternatives for the **libdwarf-tools dwarfdump** program are the **binutils readelf** program or the **elfutils eu-readelf** program, both used by passing the **--debug-dump** flag.

(BZ#1920624)

The gdb.i686 packages are deprecated

In RHEL 8.1, the 32-bit versions of the GNU Debugger (GDB), **gdb.i686**, were shipped due to a dependency problem in another package. Because RHEL 8 does not support 32-bit hardware, the **gdb.i686** packages are deprecated since RHEL 8.4. The 64-bit versions of GDB, **gdb.x86_64**, are fully capable of debugging 32-bit applications.

If you use **gdb.i686** note the following important issues:

- The **gdb.i686** packages will no longer be updated. Users must install **gdb.x86_64** instead.
- If you have **gdb.i686** installed, installing **gdb.x86_64** will cause **dnf** to report **package gdb-8.2-**

14.el8.x86_64 obsoletes gdb < 8.2-14.el8 provided by gdb-8.2-12.el8.i686. This is expected. Either uninstall **gdb.i686** or pass **dnf** the **--allowerasing** option to remove **gdb.i686** and install **gdb.x8_64**.

- Users will no longer be able to install the **gdb.i686** packages on 64-bit systems, that is, those with the **libc.so.6()(64-bit)** packages.

(BZ#1853140)

7.10. IDENTITY MANAGEMENT

openssh-ldap has been deprecated

The **openssh-ldap** subpackage has been deprecated in Red Hat Enterprise Linux 8 and will be removed in RHEL 9. As the **openssh-ldap** subpackage is not maintained upstream, Red Hat recommends using SSSD and the **sss_ssh_authorizedkeys** helper, which integrate better with other IdM solutions and are more secure.

By default, the SSSD **ldap** and **ipa** providers read the **sshPublicKey** LDAP attribute of the user object, if available. Note that you cannot use the default SSSD configuration for the **ad** provider or IdM trusted domains to retrieve SSH public keys from Active Directory (AD), since AD does not have a default LDAP attribute to store a public key.

To allow the **sss_ssh_authorizedkeys** helper to get the key from SSSD, enable the **ssh** responder by adding **ssh** to the **services** option in the **sssd.conf** file. See the **sssd.conf(5)** man page for details.

To allow **sshd** to use **sss_ssh_authorizedkeys**, add the **AuthorizedKeysCommand /usr/bin/sss_ssh_authorizedkeys** and **AuthorizedKeysCommandUser nobody** options to the **/etc/ssh/sshd_config** file as described by the **sss_ssh_authorizedkeys(1)** man page.

(BZ#1871025)

DES and 3DES encryption types have been removed

Due to security reasons, the Data Encryption Standard (DES) algorithm has been deprecated and disabled by default since RHEL 7. With the recent rebase of Kerberos packages, single-DES (DES) and triple-DES (3DES) encryption types have been removed from RHEL 8.

If you have configured services or users to only use DES or 3DES encryption, you might experience service interruptions such as:

- Kerberos authentication errors
- **unknown enctype** encryption errors
- Kerberos Distribution Centers (KDCs) with DES-encrypted Database Master Keys (**K/M**) fail to start

Perform the following actions to prepare for the upgrade:

1. Check if your KDC uses DES or 3DES encryption with the **krb5check** open source Python scripts. See krb5check on GitHub.
2. If you are using DES or 3DES encryption with any Kerberos principals, re-key them with a supported encryption type, such as Advanced Encryption Standard (AES). For instructions on re-keying, see Retiring DES from MIT Kerberos Documentation.

3. Test independence from DES and 3DES by temporarily setting the following Kerberos options before upgrading:
   a. In **/var/kerberos/krb5kdc/kdc.conf** on the KDC, set **supported_enctypes** and do not include **des** or **des3**.
   b. For every host, in **/etc/krb5.conf** and any files in **/etc/krb5.conf.d**, set **allow_weak_crypto** to **false**. It is false by default.
   c. For every host, in **/etc/krb5.conf** and any files in **/etc/krb5.conf.d**, set **permitted_enctypes**, **default_tgs_enctypes**, and **default_tkt_enctypes** and do not include **des** or **des3**.
4. If you do not experience any service interruptions with the test Kerberos settings from the previous step, remove them and upgrade. You do not need those settings after upgrading to the latest Kerberos packages.

(BZ#1877991)

Standalone use of the ctdb service has been deprecated

Since RHEL 8.4, customers are advised to use the **ctdb** clustered Samba service only when both of the following conditions apply:

- The **ctdb** service is managed as a **pacemaker** resource with the resource-agent **ctdb**.
- The **ctdb** service uses storage volumes that contain either a GlusterFS file system provided by the Red Hat Gluster Storage product or a GFS2 file system.

The stand-alone use case of the **ctdb** service has been deprecated and will not be included in a next major release of Red Hat Enterprise Linux. For further information on support policies for Samba, see the Knowledgebase article Support Policies for RHEL Resilient Storage - ctdb General Policies .

(BZ#1916296)

Running Samba as a PDC or BDC is deprecated

The classic domain controller mode that enabled administrators to run Samba as an NT4-like primary domain controller (PDC) and backup domain controller (BDC) is deprecated. The code and settings to configure these modes will be removed in a future Samba release.

As long as the Samba version in RHEL 8 provides the PDC and BDC modes, Red Hat supports these modes only in existing installations with Windows versions which support NT4 domains. Red Hat recommends not setting up a new Samba NT4 domain, because Microsoft operating systems later than Windows 7 and Windows Server 2008 R2 do not support NT4 domains.

If you use the PDC to authenticate only Linux users, Red Hat suggests migrating to Red Hat Identity Management (IdM) that is included in RHEL subscriptions. However, you cannot join Windows systems to an IdM domain. Note that Red Hat continues supporting the PDC functionality IdM uses in the background.

Red Hat does not support running Samba as an AD domain controller (DC).

(BZ#1926114)

The SSSD version of libwbclient has been removed

The SSSD implementation of the **libwbclient** package was deprecated in RHEL 8.4. As it cannot be used with recent versions of Samba, the SSSD implementation of **libwbclient** has now been removed.

(BZ#1947671)

7.11. DESKTOP

The libgnome-keyring library has been deprecated

The **libgnome-keyring** library has been deprecated in favor of the **libsecret** library, as **libgnome-keyring** is not maintained upstream, and does not follow the necessary cryptographic policies for RHEL. The new **libsecret** library is the replacement that follows the necessary security standards.

(BZ#1607766)

7.12. GRAPHICS INFRASTRUCTURES

AGP graphics cards are no longer supported

Graphics cards using the Accelerated Graphics Port (AGP) bus are not supported in Red Hat Enterprise Linux 8. Use the graphics cards with PCI-Express bus as the recommended replacement.

(BZ#1569610)

Motif is deprecated

The Motif widget toolkit is now deprecated. Development in the upstream Motif community is inactive.

The following Motif packages are deprecated, including their development and debugging variants:

- **motif**
- **motif-static**
- **openmotif**
- **openmotif21**
- **openmotif22**

Red Hat recommends using the GTK toolkit as a replacement. GTK is more maintainable and provides new features compared to Motif.

(JIRA:RHELPLAN-98983)

7.13. THE WEB CONSOLE

The web console no longer supports incomplete translations

The RHEL web console no longer provides translations for languages that have translations available for less than 50 % of the Console’s translatable strings. If the browser requests translation to such a language, the user interface will be in English instead.

(BZ#1666722)

7.14. RED HAT ENTERPRISE LINUX SYSTEM ROLES

The geoipupdate package has been deprecated

The **geoipupdate** package requires a third-party subscription and it also downloads proprietary content. Therefore, the **geoipupdate** package has been deprecated, and will be removed in the next major RHEL version.

(BZ#1874892)

7.15. VIRTUALIZATION

virt-manager has been deprecated

The Virtual Machine Manager application, also known as **virt-manager**, has been deprecated. The RHEL 8 web console, also known as **Cockpit**, is intended to become its replacement in a subsequent release. It is, therefore, recommended that you use the web console for managing virtualization in a GUI. Note, however, that some features available in **virt-manager** may not be yet available the RHEL 8 web console.

(JIRA:RHELPLAN-10304)

Virtual machine snapshots are not properly supported in RHEL 8

The current mechanism of creating virtual machine (VM) snapshots has been deprecated, as it is not working reliably. As a consequence, it is recommended not to use VM snapshots in RHEL 8.

(BZ#1686057)

The Cirrus VGA virtual GPU type has been deprecated

With a future major update of Red Hat Enterprise Linux, the **Cirrus VGA** GPU device will no longer be supported in KVM virtual machines. Therefore, Red Hat recommends using the **stdvga**, **virtio-vga**, or **qxl** devices instead of Cirrus VGA.

(BZ#1651994)

KVM on IBM POWER has been deprecated

Using KVM virtualization on IBM POWER hardware has become deprecated. As a result, KVM on IBM POWER is still supported in RHEL 8, but will become unsupported in a future major release of RHEL.

(JIRA:RHELPLAN-71200)

SecureBoot image verification using SHA1-based signatures is deprecated

Performing SecureBoot image verification using SHA1-based signatures on UEFI (PE/COFF) executables has become deprecated.

Instead, Red Hat recommends using signatures based on the SHA2 algorithm, or later.

(BZ#1935497)

SPICE has been deprecated

The SPICE remote display protocol has become deprecated. Note that SPICE will remain supported in RHEL 8, but Red Hat recommends using alternate solutions for remote display streaming:

- For remote console access, use the VNC protocol.
- For advanced remote display functions, use third party tools such as RDP, HP RGS, or Mechdyne TGX.

(BZ#1849563)

7.16. CONTAINERS

The Podman varlink-based API v1.0 has been removed

The Podman varlink-based API v1.0 was deprecated in a previous release of RHEL 8. Podman v2.0 introduced a new Podman v2.0 RESTful API. With the release of Podman v3.0, the varlink-based API v1.0 has been completely removed.

(JIRA:RHELPLAN-45858)

container-tools:1.0 has been deprecated

The **container-tools:1.0** module has been deprecated and will no longer receive security updates. It is recommended to use a newer supported stable module stream, such as **container-tools:2.0** or **container-tools:3.0**.

(JIRA:RHELPLAN-59825)

7.17. DEPRECATED PACKAGES

The following packages have been deprecated and will probably not be included in a future major release of Red Hat Enterprise Linux:

- 389-ds-base-legacy-tools
- antlr3
- aopalliance
- apache-commons-collections
- apache-commons-compress
- apache-commons-jxpath
- apiguardian
- authd
- auto
- base64coder
- batik
- bea-stax
- bea-stax-api
- bouncycastle
- cal10n
- cbi-plugins

- cdrdao
- codehaus-parent
- compat-libpthread-nonshared
- compat-openssl10
- custodia
- drpm
- dvd+rw-tools
- dyninst-static
- eclipse-ecf
- eclipse-emf
- eclipse-license
- ed25519-java
- ee4j-parent
- elfutils-devel-static
- elfutils-libelf-devel-static
- environment-modules-compat
- fipscheck
- fipscheck-lib
- forge-parent
- future
- genwqe-vpd
- genwqe-zlib
- genwqe-zlib-devel
- geoipupdate
- geronimo-annotation
- geronimo-jpa
- glassfish-annotation-api
- glassfish-el
- glassfish-fastinfoset

- glassfish-jaxb-core
- glassfish-jaxb-txw2
- glassfish-jsp
- glassfish-jsp-api
- glassfish-servlet-api
- gnupg2-smime
- google-gson
- gssntlmssp
- guile
- hawtjni
- hawtjni
- highlight-gui
- hostname
- icu4j
- iptables
- ipython
- isl
- isl-devel
- isorelax
- istack-commons-runtime
- istack-commons-tools
- iwl3945-firmware
- iwl4965-firmware
- iwl6000-firmware
- jacoco
- jaf
- janino
- jansi-native
- jarjar

- java-atk-wrapper
- javaewah
- javaparser
- javapoet
- javassist
- jaxen
- jboss-annotations-1.2-api
- jboss-interceptors-1.2-api
- jboss-logmanager
- jctools
- jetty
- jffi
- jgit
- jline
- jnr-netdb
- jolokia-jvm-agent
- js-uglify
- jsch
- json_simple
- jss-javadoc
- jtidy
- junit5
- jzlib
- ldapjdk-javadoc
- libblocksruntime
- libcacard
- libcacard-devel
- libcgroup
- libidn

- libdnet
- libdwarf
- libdwarf-devel
- libdwarf-static
- libdwarf-tools
- libertas-sd8686-firmware
- libertas-usb8388-firmware
- libertas-usb8388-olpc-firmware
- libgovirt
- libguestfs-benchmarking
- libguestfs-gfs2
- libguestfs-java
- libguestfs-java-devel
- libguestfs-javadoc
- libguestfs-tools
- libguestfs-tools-c
- libhugetlbfs
- libhugetlbfs-devel
- libhugetlbfs-utils
- libidn
- libiscsi-devel
- liblogging
- libmcpp
- libmemcached
- libmetalink
- libmodulemd1
- libmongocrypt
- libmusicbrainz5
- liboauth

- liboauth-devel
- libpfm-static
- libpng12
- libselinux-python
- libsqlite3x
- libtar
- libunwind
- libvarlink
- libvirt-admin
- libvirt-bash-completion
- libvirt-daemon-driver-storage-gluster
- libvirt-daemon-driver-storage-iscsi-direct
- libvirt-gconfig
- libvirt-gobject
- libyami
- log4j12
- lorax-composer
- lucene
- mailman
- mailx - replaced by s-nail
- make-devel
- maven-install-plugin
- maven-scm
- maven2
- mercurial
- mingw32-bzip2-static
- mongo-c-driver
- msv-javadoc
- msv-manual

- nbdkit-gzip-plugin
- ncompress
- net-tools
- netcf
- netcf-devel
- netcf-libs
- network-scripts
- nss_nis
- nss-pam-ldapd
- objectweb-asm
- objectweb-pom
- ocaml-bisect-ppx
- opencv-contrib
- opencv-core
- openhpi
- openhpi-libs
- openssh-cavs
- openssh-ldap
- openssl-ibmpkcs11
- opentest4j
- parfait
- parfait-examples
- parfait-javadoc
- pcp-parfait-agent
- pcp-pmda-rpm
- pcsc-lite-doc
- peripety
- perl-B-Debug
- perl-B-Lint

- perl-File-CheckTree
- perl-libxml-perl
- perl-Locale-Codes
- perl-prefork
- perl-Sys-Virt
- pinentry-emacs
- pinentry-gtk
- plexus-component-api
- python-nss-doc
- python-redis
- python-schedutils
- python-varlink
- python2-mock
- python3-click
- python3-cpio
- python3-custodia
- python3-flask
- python3-gevent
- python3-html5lib
- python3-itsdangerous
- python3-jwt
- python3-networkx-core
- python3-nose
- python3-nss
- python3-pillow
- python3-pydbus
- python3-pymongo
- python3-pytoml - replaced by python3-toml
- python3-schedutils

- python3-syspurpose
- python3-virtualenv - use the **venv** module in Python 3 instead
- python3-webencodings
- python3-werkzeug
- qemu-kvm-block-gluster
- qemu-kvm-block-iscsi
- qpid-proton
- qt5-qtcanvas3d
- qt5-qtcanvas3d-examples
- redhat-support-lib-python
- redhat-support-tool
- reflections
- relaxngDatatype
- rhsm-gtk
- rsyslog-udpspoof
- rubygem-abrt
- rubygem-abrt-doc
- SDL_sound
- selinux-policy-minimum
- scala
- sendmail
- sgabios
- sgabios-bin
- shrinkwrap
- SLOF
- spice-client-win-x64
- spice-client-win-x86
- spice-glib
- spice-glib-devel

- spice-gtk
- spice-gtk-tools
- spice-gtk3
- spice-gtk3-devel
- spice-gtk3-vala
- spice-parent
- spice-qxl-wddm-dod
- spice-streaming-agent
- spice-vdagent-win-x64
- spice-vdagent-win-x86
- stax-ex
- stax2-api
- stringtemplate4
- subscription-manager-initial-setup-addon
- subscription-manager-migration
- subscription-manager-migration-data
- system-storage-manager
- trousers
- uglify-js
- univocity-parsers
- usbguard-notifier
- velocity
- virt-dib
- virt-p2v-maker
- vm-dump-metrics-devel
- weld-parent
- woodstox-core
- xdelta
- xmlgraphics-commons

- xmlstreambuffer
- xorg-x11-drv-qxl
- xorg-x11-server-Xspice
- xpp3
- xsom
- xz-java
- yp-tools
- ypbind
- ypserv

7.18. DEPRECATED DEVICES

This section lists devices (drivers, adapters) that continue to be supported until the end of life of RHEL 8 but will likely not be supported in future major releases of this product and are not recommended for new deployments. Support for devices other than those listed remains unchanged.

PCI IDs are in the format of *vendor:device:subvendor:subdevice*. If the *subdevice* or *subvendor:subdevice* entry is not listed, devices with any values of such missing entries have been deprecated. To check the PCI IDs of the hardware on your system, run the **lspci -nn** command.

Device type	Driver	Device	Device ID
PCI	bnx2		
PCI	hpsa		0x103C:0x3239:0x103C:0x21C4
PCI	hpsa		0x103C:0x3239:0x103C:0x21C9
PCI	hpsa		0x103C:0x3239:0x103C:0x21CC
PCI	hpsa		0x103C:0x3239:0x103C:0x21CD
PCI	hpsa		0x103C:0x3239:0x103C:0x21CE
PCI	hpsa		0x103C:0x323a:0x103C:0x3233
PCI	hpsa		0x103C:0x323a:0x103C:0x3241
PCI	hpsa		0x103C:0x323a:0x103C:0x3243
PCI	hpsa		0x103C:0x323a:0x103C:0x3245

Device type	Driver	Device	Device ID
PCI	hpsa		0x103C:0x323a:0x103C:0x3247
PCI	hpsa		0x103C:0x323a:0x103C:0x3249
PCI	hpsa		0x103C:0x323a:0x103C:0x324A
PCI	hpsa		0x103C:0x323a:0x103C:0x324B
PCI	hpsa		0x103C:0x323b:0x103C:0x3350
PCI	hpsa		0x103C:0x323b:0x103C:0x3351
PCI	hpsa		0x103C:0x323b:0x103C:0x3352
PCI	hpsa		0x103C:0x323b:0x103C:0x3353
PCI	hpsa		0x103C:0x323b:0x103C:0x3354
PCI	hpsa		0x103C:0x323b:0x103C:0x3355
PCI	hpsa		0x103C:0x323b:0x103C:0x3356
PCI	hpsa		0x103C:0x333f:0x103c:0x333f
PCI	hpsa		0x9005:0x0290:0x9005:0x0580
PCI	hpsa		0x9005:0x0290:0x9005:0x0581
PCI	hpsa		0x9005:0x0290:0x9005:0x0582
PCI	hpsa		0x9005:0x0290:0x9005:0x0583
PCI	hpsa		0x9005:0x0290:0x9005:0x0584
PCI	hpsa		0x9005:0x0290:0x9005:0x0585
PCI	lpfc		0x10df:0x0724
PCI	lpfc		0x10df:0xe200
PCI	lpfc		0x10df:0xe220
PCI	lpfc		0x10df:0xf011

Device type	Driver	Device	Device ID
PCI	lpfc		0x10df:0xf015
PCI	lpfc		0x10df:0xf100
PCI	lpfc		0x10df:0xfc40
PCI	megaraid_sas		0x1000:0x005b
PCI	mpt3sas		0x1000:0x006E
PCI	mpt3sas		0x1000:0x0080
PCI	mpt3sas		0x1000:0x0081
PCI	mpt3sas		0x1000:0x0082
PCI	mpt3sas		0x1000:0x0083
PCI	mpt3sas		0x1000:0x0084
PCI	mpt3sas		0x1000:0x0085
PCI	mpt3sas		0x1000:0x0086
PCI	mpt3sas		0x1000:0x0087
PCI	myri10ge		
PCI	netxen_nic		
PCI	sfc		0x1924:0x0803
PCI	sfc		0x1924:0x0813
PCI	qla2xxx		0x1077:0x2031
PCI	qla2xxx		0x1077:0x2532
PCI	qla2xxx		0x1077:0x8031

CHAPTER 8. KNOWN ISSUES

This part describes known issues in Red Hat Enterprise Linux 8.5 Beta.

8.1. INSTALLER AND IMAGE CREATION

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

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

To work around this problem, use the **harddrive --partition=sdX --dir=/** command to install from USB CD-ROM drive. As a result, the installation does not fail.

(BZ#1914955)

Anaconda does not show encryption for a custom partition

The **Encrypt my data** radio button is not available when you choose the **Custom** partitioning during the system installation. As a result, your data is not encrypted when installation is complete.

To workaround this problem, set encryption in the custom partitioning screen for each device you want to encrypt. Anaconda will ask for a passphrase when leaving the dialog.

(BZ#1903786)

Installation program attempts automatic partitioning when no partitioning scheme is specified in the Kickstart file

When using a Kickstart file to perform an automated installation, the installation program attempts to perform automatic partitioning even when you do not specify any partitioning commands in the Kickstart file. The installation program behaves as if the **autopart** command was used in the Kickstart file, resulting in unexpected partitions. To work around this problem, use the **reqpart** command in the Kickstart file so that you can interactively configure manual partitioning.

(BZ#1954408)

The auth and authconfig Kickstart commands require the AppStream repository

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

To work around this problem, verify that the BaseOS and AppStream repositories are available to the installer or use the **authselect** Kickstart command during installation.

(BZ#1640697)

The reboot --kexec and inst.kexec commands do not provide a predictable system state

Performing a RHEL installation with the **reboot --kexec** Kickstart command or the **inst.kexec** kernel boot parameters do not provide the same predictable system state as a full reboot. As a consequence, switching to the installed system without rebooting can produce unpredictable results.

Note that the **kexec** feature is deprecated and will be removed in a future release of Red Hat Enterprise Linux.

(BZ#1697896)

Network access is not enabled by default in the installation program

Several installation features require network access, for example, registration of a system using the Content Delivery Network (CDN), NTP server support, and network installation sources. However, network access is not enabled by default, and as a result, these features cannot be used until network access is enabled.

To work around this problem, add **ip=dhcp** to boot options to enable network access when the installation starts. Optionally, passing a Kickstart file or a repository located on the network using boot options also resolves the problem. As a result, the network-based installation features can be used.

(BZ#1757877)

Adding the same username in both blueprint and Kickstart files causes Edge image installation to fail

To install a RHEL for Edge image, users must create a blueprint to build a **rhel-edge-container image** and also create a Kickstart file to install the RHEL for Edge image. When a user adds the same username, password, and SSH key in both the blueprint and the Kickstart file, the RHEL for Edge image installation fails. Currently, there is no workaround.

(BZ#1951964)

The new **osbuild-composer** back end does not replicate the blueprint state from **lorax-composer** on upgrades

Image Builder users that are upgrading from the **lorax-composer** back end to the new **osbuild-composer** back end, blueprints can disappear. As a result, once the upgrade is complete, the blueprints do not display automatically. To work around this problem, perform the following steps.

Prerequisites

- You have the **composer-cli** CLI utility installed.

Procedure

1. Run the command to load the previous **lorax-composer** based blueprints into the new **osbuild-composer** back end:

```
$ for blueprint in $(find /var/lib/lorax/composer/blueprints/git/workspace/master -name
'*.toml'); do composer-cli blueprints push "${blueprint}"; done
```

As a result, the same blueprints are now available in **osbuild-composer** back end.

Additional resources

- For more details about this Known Issue, see the Image Builder blueprints are no longer present following an update to Red Hat Enterprise Linux 8.3 article.

(BZ#1897383)

GUI installation might fail if an attempt to unregister using the CDN is made before the repository refresh is completed

Since RHEL 8.2, when registering your system and attaching subscriptions using the Content Delivery Network (CDN), a refresh of the repository metadata is started by the GUI installation program. The refresh process is not part of the registration and subscription process, and as a consequence, the

Unregister button is enabled in the **Connect to Red Hat** window. Depending on the network connection, the refresh process might take more than a minute to complete. If you click the **Unregister** button before the refresh process is completed, the GUI installation might fail as the unregister process removes the CDN repository files and the certificates required by the installation program to communicate with the CDN.

To work around this problem, complete the following steps in the GUI installation after you have clicked the **Register** button in the **Connect to Red Hat** window:

1. From the **Connect to Red Hat** window, click **Done** to return to the **Installation Summary** window.
2. From the **Installation Summary** window, verify that the **Installation Source** and **Software Selection** status messages in italics are not displaying any processing information.
3. When the Installation Source and Software Selection categories are ready, click **Connect to Red Hat**.
4. Click the **Unregister** button.

After performing these steps, you can safely unregister the system during the GUI installation.

(BZ#1821192)

Registration fails for user accounts that belong to multiple organizations

Currently, when you attempt to register a system with a user account that belongs to multiple organizations, the registration process fails with the error message **You must specify an organization for new units**.

To work around this problem, you can either:

- Use a different user account that does not belong to multiple organizations.
- Use the **Activation Key** authentication method available in the Connect to Red Hat feature for GUI and Kickstart installations.
- Skip the registration step in Connect to Red Hat and use Subscription Manager to register your system post-installation.

(BZ#1822880)

8.2. SUBSCRIPTION MANAGEMENT

syspurpose addons have no effect on the **subscription-manager attach --auto** output.

In Red Hat Enterprise Linux 8, four attributes of the **syspurpose** command-line tool have been added: **role**,**usage**, **service_level_agreement** and **addons**. Currently, only **role**, **usage** and **service_level_agreement** affect the output of running the **subscription-manager attach --auto** command. Users who attempt to set values to the **addons** argument will not observe any effect on the subscriptions that are auto-attached.

(BZ#1687900)

8.3. SOFTWARE MANAGEMENT

libdnf-devel upgrade fails if the CodeReady Linux Builder repository is not available on the system

The **libdnf-devel** package has been moved from the BaseOS to CodeReady Linux Builder repository. Consequently, upgrading **libdnf-devel** fails if the CodeReady Linux Builder repository is not available on the system.

To work around this problem, enable the CodeReady Linux Builder repository, or remove the **libdnf-devel** package prior to the upgrade.

(BZ#1960616)

cr_compress_file_with_stat() can cause a memory leak

The **createrepo_c** library has the API **cr_compress_file_with_stat()** function. This function is declared with **char **dst** as a second parameter. Depending on its other parameters, **cr_compress_file_with_stat()** either uses **dst** as an input parameter, or uses it to return an allocated string. This unpredictable behavior can cause a memory leak, because it does not inform the user when to free **dst** contents.

To work around this problem, a new API **cr_compress_file_with_stat_v2** function has been added, which uses the **dst** parameter only as an input. It is declared as **char *dst**. This prevents memory leak.

Note that the **cr_compress_file_with_stat_v2** function is temporary and will be present only in RHEL 8. Later, **cr_compress_file_with_stat()** will be fixed instead.

(BZ#1973588)

8.4. INFRASTRUCTURE SERVICES

Postfix TLS fingerprint algorithm in the FIPS mode needs to be changed to SHA-256

By default in RHEL 8, **postfix** uses MD5 fingerprints with the TLS for backward compatibility. But in the FIPS mode, the MD5 hashing function is not available, which may cause TLS to incorrectly function in the default postfix configuration. To workaround this problem, the hashing function needs to be changed to SHA-256 in the postfix configuration file.

For more details, see the related Knowledgebase article Fix postfix TLS in the FIPS mode by switching to SHA-256 instead of MD5.

(BZ#1711885)

8.5. SECURITY

File permissions of **/etc/passwd-** are not aligned with the CIS RHEL 8 Benchmark 1.0.0

Because of an issue with the CIS Benchmark, the remediation of the SCAP rule that ensures permissions on the **/etc/passwd-** backup file configures permissions to **0644**. However, the **CIS Red Hat Enterprise Linux 8 Benchmark 1.0.0** requires file permissions **0600** for that file. As a consequence, the file permissions of **/etc/passwd-** are not aligned with the benchmark after remediation.

(BZ#1858866)

libselinux-python is available only through its module

The **libselinux-python** package contains only Python 2 bindings for developing SELinux applications and it is used for backward compatibility. For this reason, **libselinux-python** is no longer available in the default RHEL 8 repositories through the **dnf install libselinux-python** command.

To work around this problem, enable both the **libselinux-python** and **python27** modules, and install the **libselinux-python** package and its dependencies with the following commands:

```
# dnf module enable libselinux-python
# dnf install libselinux-python
```

Alternatively, install **libselinux-python** using its install profile with a single command:

```
# dnf module install libselinux-python:2.8/common
```

As a result, you can install **libselinux-python** using the respective module.

(BZ#1666328)

udica processes UBI 8 containers only when started with **--env container=podman**

The Red Hat Universal Base Image 8 (UBI 8) containers set the **container** environment variable to the **oci** value instead of the **podman** value. This prevents the **udica** tool from analyzing a container JavaScript Object Notation (JSON) file.

To work around this problem, start a UBI 8 container using a **podman** command with the **--env container=podman** parameter. As a result, **udica** can generate an SELinux policy for a UBI 8 container only when you use the described workaround.

(BZ#1763210)

Negative effects of the default logging setup on performance

The default logging environment setup might consume 4 GB of memory or even more and adjustments of rate-limit values are complex when **systemd-journald** is running with **rsyslog**.

See the Negative effects of the RHEL default logging setup on performance and their mitigations Knowledgebase article for more information.

(JIRA:RHELPLAN-10431)

SELINUX=disabled in **/etc/selinux/config** does not work properly

Disabling SELinux using the **SELINUX=disabled** option in the **/etc/selinux/config** results in a process in which the kernel boots with SELinux enabled and switches to disabled mode later in the boot process. This might cause memory leaks.

To work around this problem, disable SELinux by adding the **selinux=0** parameter to the kernel command line as described in the Changing SELinux modes at boot time section of the Using SELinux title if your scenario really requires to completely disable SELinux.

(JIRA:RHELPLAN-34199)

crypto-policies incorrectly allow Camellia ciphers

The RHEL 8 system-wide cryptographic policies should disable Camellia ciphers in all policy levels, as stated in the product documentation. However, the Kerberos protocol enables the ciphers by default.

To work around the problem, apply the **NO-CAMELLIA** subpolicy:

```
# update-crypto-policies --set DEFAULT:NO-CAMELLIA
```

In the previous command, replace **DEFAULT** with the cryptographic level name if you have switched from **DEFAULT** previously.

As a result, Camellia ciphers are correctly disallowed across all applications that use system-wide crypto policies only when you disable them through the workaround.

(BZ#1919155)

Using multiple labeled IPsec connections with IKEv2 do not work correctly

When Libreswan uses the **IKEv2** protocol, security labels for IPsec do not work correctly for more than one connection. As a consequence, Libreswan using labeled IPsec can establish only the first connection, but cannot establish subsequent connections correctly. To use more than one connection, use the **IKEv1** protocol.

(BZ#1934859)

Smart-card provisioning process through OpenSC pkcs15-init does not work properly

The **file_caching** option is enabled in the default OpenSC configuration, and the file caching functionality does not handle some commands from the **pkcs15-init** tool properly. Consequently, the smart-card provisioning process through OpenSC fails.

To work around the problem, add the following snippet to the **/etc/opensc.conf** file:

```
app pkcs15-init {
        framework pkcs15 {
                use_file_caching = false;
        }
}
```

The smart-card provisioning through **pkcs15-init** only works if you apply the previously described workaround.

(BZ#1947025)

Connections to servers with SHA-1 signatures do not work with GnuTLS

SHA-1 signatures in certificates are rejected by the GnuTLS secure communications library as insecure. Consequently, applications that use GnuTLS as a TLS backend cannot establish a TLS connection to peers that offer such certificates. This behavior is inconsistent with other system cryptographic libraries.

To work around this problem, upgrade the server to use certificates signed with SHA-256 or stronger hash, or switch to the LEGACY policy.

(BZ#1628553)

OpenSSL in FIPS mode accepts only specific D-H parameters

In FIPS mode, TLS clients that use OpenSSL return a **bad dh value** error and abort TLS connections to servers that use manually generated parameters. This is because OpenSSL, when configured to work in compliance with FIPS 140-2, works only with Diffie-Hellman parameters compliant to NIST SP 800-56A rev3 Appendix D (groups 14, 15, 16, 17, and 18 defined in RFC 3526 and with groups defined in RFC 7919). Also, servers that use OpenSSL ignore all other parameters and instead select known parameters of similar size. To work around this problem, use only the compliant groups.

(BZ#1810911)

IKE over TCP connections do not work on custom TCP ports

The **tcp-remoteport** Libreswan configuration option does not work properly. Consequently, an IKE over TCP connection cannot be established when a scenario requires specifying a non-default TCP port.

(BZ#1989050)

Conflict in SELinux Audit rules and SELinux boolean configurations

If the Audit rule list includes an Audit rule that contains a **subj_*** or **obj_*** field, and the SELinux boolean configuration changes, setting the SELinux booleans causes a deadlock. As a consequence, the system stops responding and requires a reboot to recover. To work around this problem, disable all Audit rules containing the **subj_*** or **obj_*** field, or temporarily disable such rules before changing SELinux booleans.

With the release of the RHSA-2021:2168 advisory, the kernel handles this situation properly and no longer deadlocks.

(BZ#1924230)

Certain sets of interdependent rules in SSG can fail

Remediation of **SCAP Security Guide** (SSG) rules in a benchmark can fail due to undefined ordering of rules and their dependencies. If two or more rules need to be executed in a particular order, for example, when one rule installs a component and another rule configures the same component, they can run in the wrong order and remediation reports an error. To work around this problem, run the remediation twice, and the second run fixes the dependent rules.

(BZ#1750755)

Remediating service-related rules during kickstart installations might fail

During a kickstart installation, the OpenSCAP utility sometimes incorrectly shows that a service **enable** or **disable** state remediation is not needed. Consequently, OpenSCAP might set the services on the installed system to a non-compliant state. As a workaround, you can scan and remediate the system after the kickstart installation. This will fix the service-related issues.

(BZ#1834716)

Installation with the **Server with GUI** or **Workstation** software selections and CIS security profile is not possible

The CIS security profile is not compatible with the **Server with GUI** and **Workstation** software selections. As a consequence, a RHEL 8 installation with the **Server with GUI** software selection and CIS profile is not possible. An attempted installation using the CIS profile and either of these software selections will generate the error message:

> package xorg-x11-server-common has been added to the list of excluded packages, but it can't be removed from the current software selection without breaking the installation.

To work around the problem, do not use the CIS security profile with the **Server with GUI** or **Workstation** software selections.

(BZ#1843932)

Kickstart uses **org_fedora_oscap** instead of **com_redhat_oscap** in RHEL 8

The Kickstart references the Open Security Content Automation Protocol (OSCAP) Anaconda add-on as **org_fedora_oscap** instead of **com_redhat_oscap** which might cause confusion. That is done to preserve backward compatibility with Red Hat Enterprise Linux 7.

(BZ#1665082)

usbguard-notifier logs too many error messages to the Journal

The **usbguard-notifier** service does not have inter-process communication (IPC) permissions for connecting to the **usbguard-daemon** IPC interface. Consequently, **usbguard-notifier** fails to connect to the interface, and it writes a corresponding error message to the Journal. Because **usbguard-notifier** starts with the **--wait** option, which ensures that **usbguard-notifier** attempts to connect to the IPC interface each second after a connection failure, by default, the log contains an excessive amount of these messages soon.

To work around the problem, allow a user or a group under which **usbguard-notifier** is running to connect to the IPC interface. For example, the following error message contains the UID and GID values for the GNOME Display Manager (GDM):

```
IPC connection denied: uid=42 gid=42 pid=8382, where uid and gid 42 = gdm
```

To grant the missing permissions to the **gdm** user, use the **usbguard** command and restart the **usbguard** daemon:

```
# usbguard add-user gdm --group --devices listen
# systemctl restart usbguard
```

After granting the missing permissions, the error messages no longer appear in the log.

(BZ#2000000)

Certain **rsyslog** priority strings do not work correctly

Support for the **GnuTLS** priority string for **imtcp** that allows fine-grained control over encryption is not complete. Consequently, the following priority strings do not work properly in **rsyslog**:

```
NONE:+VERS-ALL:-VERS-TLS1.3:+MAC-ALL:+DHE-RSA:+AES-256-GCM:+SIGN-RSA-
SHA384:+COMP-ALL:+GROUP-ALL
```

To work around this problem, use only correctly working priority strings:

```
NONE:+VERS-ALL:-VERS-TLS1.3:+MAC-ALL:+ECDHE-RSA:+AES-128-CBC:+SIGN-RSA-
SHA1:+COMP-ALL:+GROUP-ALL
```

As a result, current configurations must be limited to the strings that work correctly.

(BZ#1679512)

8.6. NETWORKING

NetworkManager does not support activating bond and team ports in a specific order

NetworkManager activates interfaces alphabetically by interface names. However, if an interface appears later during the boot, for example, because the kernel needs more time to discover it, NetworkManager activates this interface later. NetworkManager does not support setting a priority on bond and team ports. Consequently, the order in which NetworkManager activates ports of these devices is not always predictable. To work around this problem, write a dispatcher script. For an example of such a script, see the corresponding comment in the ticket.

(BZ#1920398)

Systems with the **IPv6_rpfilter** option enabled experience low network throughput

Systems with the **IPv6_rpfilter** option enabled in the **firewalld.conf** file currently experience suboptimal performance and low network throughput in high traffic scenarios, such as 100-Gbps links. To work around the problem, disable the **IPv6_rpfilter** option. To do so, add the following line in the **/etc/firewalld/firewalld.conf** file.

```
IPv6_rpfilter=no
```

As a result, the system performs better, but also has reduced security.

(BZ#1871860)

8.7. KERNEL

Systems with a large amount of persistent memory experience delays during the boot process

Systems with a large amount of persistent memory take a long time to boot because the initialization of the memory is serialized. Consequently, if there are persistent memory file systems listed in the **/etc/fstab** file, the system might timeout while waiting for devices to become available. To work around this problem, configure the **DefaultTimeoutStartSec** option in the **/etc/systemd/system.conf** file to a sufficiently large value.

(BZ#1666538)

Reloading an identical crash extension may cause segmentation faults

When you load a copy of an already loaded crash extension file, it might trigger a segmentation fault. Currently, the crash utility detects if an original file has been loaded. Consequently, due to two identical files co-existing in the crash utility, a namespace collision occurs, which triggers the crash utility to cause a segmentation fault.

You can work around the problem by loading the crash extension file only once. As a result, segmentation faults no longer occur in the described scenario.

(BZ#1906482)

vmcore capture fails after memory hot-plug or unplug operation

After performing the memory hot-plug or hot-unplug operation, the event comes after updating the device tree which contains memory layout information. Thereby the **makedumpfile** utility tries to access a non-existent physical address. The problem appears if all of the following conditions meet:

- A little-endian variant of IBM Power System runs RHEL 8.
- The **kdump** or **fadump** service is enabled on the system.

Consequently, the capture kernel fails to save **vmcore** if a kernel crash is triggered after the memory hot-plug or hot-unplug operation.

To work around this problem, restart the **kdump** service after hot-plug or hot-unplug:

```
# systemctl restart kdump.service
```

As a result, **vmcore** is successfully saved in the described scenario.

(BZ#1793389)

Debug kernel fails to boot in crash capture environment on RHEL 8

Due to the memory-intensive nature of the debug kernel, a problem occurs when the debug kernel is in use and a kernel panic is triggered. As a consequence, the debug kernel is not able to boot as the capture kernel, and a stack trace is generated instead. To work around this problem, increase the crash kernel memory as required. As a result, the debug kernel boots successfully in the crash capture environment.

(BZ#1659609)

Allocating crash kernel memory fails at boot time

On certain Ampere Altra systems, allocating the crash kernel memory during boot fails when the 32-bit region is disabled in BIOS settings. Consequently, the **kdump** service fails to start. This is caused by memory fragmentation in the region below 4 GB with no fragment being large enough to contain the crash kernel memory.

To work around this problem, enable the 32-bit memory region in BIOS as follows:

1. Open the BIOS settings on your system.

2. Open the **Chipset** menu.

3. Under **Memory Configuration**, enable the **Slave 32-bit** option.

As a result, crash kernel memory allocation within the 32-bit region succeeds and the **kdump** service works as expected.

(BZ#1940674)

kdump fails on some KVM virtual machines using default crash kernel memory

On some KVM virtual machines **kdump** fails when using the default amount of memory for **kdump** to capture the kernel crash dump. Consequently, the crash kernel displays the following error:

```
/bin/sh: error while loading shared libraries: libtinfo.so.6: cannot open shared object file: No such file
or directory
```

To workaround this problem, increase the **crashkernel=** option by a minimum of 32M to fit the size requirement for kdump. For example, the final value must be the sum of current value and 32M.

In the case of the **crashkernel=auto** parameter:

1. Check the current memory size, and increase the size by 32M as follows:

```
echo $(($(cat /sys/kernel/kexec_crash_size)/1048576+32))M
```

1. Configure the kernel **crashkernel** parameter to **crashkernel=x**, where **x** is the increased size.

(BZ#2004000)

The QAT manager leaves no spare device for LKCF

The Intel® QuickAssist Technology (QAT) manager (**qatmgr**) is a user space process, which by default uses all QAT devices in the system. As a consequence, there are no QAT devices left for the Linux Kernel Cryptographic Framework (LKCF). There is no need to work around this situation, as this behavior is expected and a majority of users will use acceleration from the user space.

(BZ#1920086)

The **tboot-1.9.12-2** utility causes a boot failure in RHEL 8

The **tboot** utility of version 1.9.12-2 causes some systems with Trusted Platform Module (TPM) 2.0 to fail to boot in legacy mode. As a consequence, the system halts once it attempts to boot from the tboot Grand Unified Bootloader (GRUB) entry. To workaround this problem, downgrade to **tboot** of version 1.9.10.

(BZ#1947839)

The kernel ACPI driver reports it has no access to a PCIe ECAM memory region

The Advanced Configuration and Power Interface (ACPI) table provided by firmware does not define a memory region on the PCI bus in the Current Resource Settings (_CRS) method for the PCI bus device. Consequently, the following warning message occurs during the system boot:

```
[    2.817152] acpi PNP0A08:00: [Firmware Bug]: ECAM area [mem 0x30000000-0x31ffffff] not reserved in ACPI namespace
[    2.827911] acpi PNP0A08:00: ECAM at [mem 0x30000000-0x31ffffff] for [bus 00-1f]
```

However, the kernel is still able to access the **0x30000000-0x31ffffff** memory region, and can assign that memory region to the PCI Enhanced Configuration Access Mechanism (ECAM) properly. You can verify that PCI ECAM works correctly by accessing the PCIe configuration space over the 256 byte offset with the following output:

```
03:00.0 Non-Volatile memory controller: Sandisk Corp WD Black 2018/PC SN720 NVMe SSD (prog-if 02 [NVM Express])
 ...
        Capabilities: [900 v1] L1 PM Substates
                L1SubCap: PCI-PM_L1.2- PCI-PM_L1.1- ASPM_L1.2+ ASPM_L1.1- L1_PM_Substates+
                          PortCommonModeRestoreTime=255us PortTPowerOnTime=10us
                L1SubCtl1: PCI-PM_L1.2- PCI-PM_L1.1- ASPM_L1.2- ASPM_L1.1-
                           T_CommonMode=0us LTR1.2_Threshold=0ns
                L1SubCtl2: T_PwrOn=10us
```

As a result, you can ignore the warning message.

For more information about the problem, see the "Firmware Bug: ECAM area **mem 0x30000000-0x31ffffff** not reserved in ACPI namespace" appears during system boot solution.

(BZ#1868526)

The **tuned-adm profile powersave** command causes the system to become unresponsive

Executing the **tuned-adm profile powersave** command leads to an unresponsive state of the Penguin Valkyrie 2000 2-socket systems with the older Thunderx (CN88xx) processors. Consequently, reboot the system to resume working. To work around this problem, avoid using the **powersave** profile if your system matches the mentioned specifications.

(BZ#1609288)

The HP NMI watchdog does not always generate a crash dump

In certain cases, the **hpwdt** driver for the HP NMI watchdog is not able to claim a non-maskable interrupt (NMI) generated by the HPE watchdog timer because the NMI was instead consumed by the **perfmon** driver.

The missing NMI is initiated by one of two conditions:

1. The **Generate NMI** button on the Integrated Lights-Out (iLO) server management software. This button is triggered by a user.
2. The **hpwdt** watchdog. The expiration by default sends an NMI to the server.

Both sequences typically occur when the system is unresponsive. Under normal circumstances, the NMI handler for both these situations calls the **kernel panic()** function and if configured, the **kdump** service generates a **vmcore** file.

Because of the missing NMI, however, **kernel panic()** is not called and **vmcore** is not collected.

In the first case (1.), if the system was unresponsive, it remains so. To work around this scenario, use the virtual **Power** button to reset or power cycle the server.

In the second case (2.), the missing NMI is followed 9 seconds later by a reset from the Automated System Recovery (ASR).

The HPE Gen9 Server line experiences this problem in single-digit percentages. The Gen10 at an even smaller frequency.

(BZ#1602962)

Connections fail when attaching a virtual function to virtual machine

Pensando network cards that use the **ionic** device driver silently accept VLAN tag configuration requests and attempt configuring network connections while attaching network virtual functions (**VF**) to a virtual machine (**VM**). Such network connections fail as this feature is not yet supported by the card's firmware.

(BZ#1930576)

The OPEN MPI library may trigger run-time failures with default PML

In OPEN Message Passing Interface (OPEN MPI) implementation 4.0.x series, Unified Communication X (UCX) is the default point-to-point communicator (PML). The later versions of OPEN MPI 4.0.x series deprecated **openib** Byte Transfer Layer (BTL).

However, OPEN MPI, when run over a **homogeneous** cluster (same hardware and software configuration), UCX still uses **openib** BTL for MPI one-sided operations. As a consequence, this may trigger execution errors. To work around this problem:

- Run the **mpirun** command using following parameters:

```
-mca btl openib -mca pml ucx -x UCX_NET_DEVICES=mlx5_ib0
```

where,

- The **-mca btl openib** parameter disables **openib** BTL
- The **-mca pml ucx** parameter configures OPEN MPI to use **ucx** PML.
- The **x UCX_NET_DEVICES=** parameter restricts UCX to use the specified devices

The OPEN MPI, when run over a **heterogeneous** cluster (different hardware and software configuration), it uses UCX as the default PML. As a consequence, this may cause the OPEN MPI jobs to run with erratic performance, unresponsive behavior, or crash failures. To work around this problem, set the UCX priority as:

- Run the **mpirun** command using following parameters:

```
-mca pml_ucx_priority 5
```

As a result, the OPEN MPI library is able to choose an alternative available transport layer over UCX.

(BZ#1866402)

The Solarflare fails to create maximum number of virtual functions (VFs)

The Solarflare NICs fail to create a maximum number of VFs due to insufficient resources. You can check the maximum number of VFs that a PCIe device can create in the **/sys/bus/pci/devices/PCI_ID/sriov_totalvfs** file. To workaround this problem, you can either adjust the number of VFs or the VF MSI interrupt value to a lower value, either from **Solarflare Boot Manager** on startup, or using Solarflare **sfboot** utility. The default VF MSI interrupt value is **8**.

- To adjust the VF MSI interrupt value using **sfboot**:

```
# sfboot vf-msix-limit=2
```

NOTE

Adjusting VF MSI interrupt value affects the VF performance.

For more information about parameters to be adjusted accordingly, see the **Solarflare Server Adapter user guide**.

(BZ#1971506)

8.8. HARDWARE ENABLEMENT

The default 7 4 1 7 printk value sometimes causes temporary system unresponsiveness

The default 7 4 1 7**printk** value allows for better debugging of the kernel activity. However, when coupled with a serial console, this **printk** setting can cause intense I/O bursts that can lead to a RHEL system becoming temporarily unresponsive. To work around this problem, we have added a new **optimize-serial-console** TuneD profile, which reduces the default **printk** value to 4 4 1 7. Users can instrument their system as follows:

```
# tuned-adm profile throughput-performance optimize-serial-console
```

Having a lower **printk** value persistent across a reboot reduces the likelihood of system hangs.

Note that this setting change comes at the expense of losing the extra debugging information.

(JIRA:RHELPLAN-28940)

8.9. FILE SYSTEMS AND STORAGE

Limitations of LVM **writecache**

The **writecache** LVM caching method has the following limitations, which are not present in the **cache** method:

- You cannot name a **writecache** logical volume when using **pvmove** commands.
- You cannot use logical volumes with **writecache** in combination with thin pools or VDO.

The following limitation also applies to the **cache** method:

- You cannot resize a logical volume while **cache** or **writecache** is attached to it.

(JIRA:RHELPLAN-27987, BZ#1798631, BZ#1808012)

The GRUB retries to access the disk after initial failures during boot

Sometimes, Storage Area Networks (SANs) fail to acknowledge the **open** and **read** disk calls. Previously, the GRUB tool used to enter into the **grub_rescue** prompt resulting in the boot failure. With this update, GRUB retries to access the disk up to 20 times after the initial call to open and read the disk fails. If the GRUB tool is still unable to open or read the disk after these attempts, it will enter into the **grub_rescue** mode.

(BZ#1987087)

LVM **mirror** devices that store a LUKS volume sometimes become unresponsive

Mirrored LVM devices with a segment type of **mirror** that store a LUKS volume might become unresponsive under certain conditions. The unresponsive devices reject all I/O operations.

To work around the issue, Red Hat recommends that you use LVM RAID 1 devices with a segment type of **raid1** instead of **mirror** if you need to stack LUKS volumes on top of resilient software-defined storage.

The **raid1** segment type is the default RAID configuration type and replaces **mirror** as the recommended solution.

To convert **mirror** devices to **raid**, see Converting a mirrored LVM device to a RAID1 device .

(BZ#1730502)

The /**boot** file system cannot be placed on LVM

You cannot place the /**boot** file system on an LVM logical volume. This limitation exists for the following reasons:

- On EFI systems, the *EFI System Partition* conventionally serves as the /**boot** file system. The uEFI standard requires a specific GPT partition type and a specific file system type for this partition.

- RHEL 8 uses the *Boot Loader Specification* (BLS) for system boot entries. This specification requires that the /**boot** file system is readable by the platform firmware. On EFI systems, the platform firmware can read only the /**boot** configuration defined by the uEFI standard.

- The support for LVM logical volumes in the GRUB 2 boot loader is incomplete. Red Hat does not plan to improve the support because the number of use cases for the feature is decreasing due to standards such as uEFI and BLS.

Red Hat does not plan to support /**boot** on LVM. Instead, Red Hat provides tools for managing system snapshots and rollback that do not need the /**boot** file system to be placed on an LVM logical volume.

(BZ#1496229)

LVM no longer allows creating volume groups with mixed block sizes

LVM utilities such as **vgcreate** or **vgextend** no longer allow you to create volume groups (VGs) where the physical volumes (PVs) have different logical block sizes. LVM has adopted this change because file systems fail to mount if you extend the underlying logical volume (LV) with a PV of a different block size.

To re-enable creating VGs with mixed block sizes, set the **allow_mixed_block_sizes=1** option in the **lvm.conf** file.

(BZ#1768536)

8.10. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS

MariaDB 10.5 does not warn about dropping a non-existent table when the OQGraph plug-in is enabled

When the **OQGraph** storage engine plug-in is loaded to the **MariaDB 10.5** server, **MariaDB** does not warn about dropping a non-existent table. In particular, when the user attempts to drop a non-existent table using the **DROP TABLE** or **DROP TABLE IF EXISTS** SQL commands, **MariaDB** neither returns an error message nor logs a warning.

Note that the **OQGraph** plug-in is provided by the **mariadb-oqgraph-engine** package, which is not installed by default.

(BZ#1944653)

PAM plug-in version 1.0 does not work in MariaDB

MariaDB 10.3 provides the Pluggable Authentication Modules (PAM) plug-in version 1.0. **MariaDB 10.5** provides the plug-in versions 1.0 and 2.0, version 2.0 is the default.

The **MariaDB** PAM plug-in version 1.0 does not work in RHEL 8. To work around this problem, use the PAM plug-in version 2.0 provided by the **mariadb:10.5** module stream.

(BZ#1942330)

getpwnam() might fail when called by a 32-bit application

When a user of NIS uses a 32-bit application that calls the **getpwnam()** function, the call fails if the **nss_nis.i686** package is missing. To work around this problem, manually install the missing package by using the **yum install nss_nis.i686** command.

(BZ#1803161)

Symbol conflicts between OpenLDAP libraries might cause crashes in **httpd**

When both the **libldap** and **libldap_r** libraries provided by OpenLDAP are loaded and used within a single process, symbol conflicts between these libraries might occur. Consequently, Apache **httpd** child processes using the PHP **ldap** extension might terminate unexpectedly if the **mod_security** or **mod_auth_openidc** modules are also loaded by the **httpd** configuration.

Since the RHEL 8.3 update to the Apache Portable Runtime (APR) library, you can work around the problem by setting the **APR_DEEPBIND** environment variable, which enables the use of the **RTLD_DEEPBIND** dynamic linker option when loading **httpd** modules. When the **APR_DEEPBIND** environment variable is enabled, crashes no longer occur in **httpd** configurations that load conflicting libraries.

(BZ#1819607)

8.11. IDENTITY MANAGEMENT

Windows Server 2008 R2 and earlier no longer supported

In RHEL 8.4 and later, Identity Management (IdM) does not support establishing trust to Active Directory with Active Directory domain controllers running Windows Server 2008 R2 or earlier versions. RHEL IdM now requires SMB encryption when establishing the trust relationship, which is only available with Windows Server 2012 or later.

(BZ#1971061)

Using the **cert-fix** utility with the **--agent-uid pkidbuser** option breaks Certificate System

Using the **cert-fix** utility with the **--agent-uid pkidbuser** option corrupts the LDAP configuration of Certificate System. As a consequence, Certificate System might become unstable and manual steps are required to recover the system.

(BZ#1729215)

FreeRADIUS silently truncates Tunnel-Passwords longer than 249 characters

If a Tunnel-Password is longer than 249 characters, the FreeRADIUS service silently truncates it. This may lead to unexpected password incompatibilities with other systems.

To work around the problem, choose a password that is 249 characters or fewer.

(BZ#1723362)

The **/var/log/lastlog** sparse file on IdM hosts can cause performance problems

During the IdM installation, a range of 200,000 UIDs from a total of 10,000 possible ranges is randomly selected and assigned. Selecting a random range in this way significantly reduces the probability of conflicting IDs in case you decide to merge two separate IdM domains in the future.

However, having high UIDs can create problems with the **/var/log/lastlog** file. For example, if a user with the UID of 1280000008 logs in to an IdM client, the local **/var/log/lastlog** file size increases to almost 400 GB. Although the actual file is sparse and does not use all that space, certain applications are not designed to identify sparse files by default and may require a specific option to handle them. For example, if the setup is complex and a backup and copy application does not handle sparse files correctly, the file is copied as if its size was 400 GB. This behavior can cause performance problems.

To work around this problem:

- In case of a standard package, refer to its documentation to identify the option that handles sparse files.
- In case of a custom application, ensure that it is able to manage sparse files such as **/var/log/lastlog** correctly.

(JIRA:RHELPLAN-59111)

FIPS mode does not support using a shared secret to establish a cross-forest trust

Establishing a cross-forest trust using a shared secret fails in FIPS mode because NTLMSSP authentication is not FIPS-compliant. To work around this problem, authenticate with an Active Directory (AD) administrative account when establishing a trust between an IdM domain with FIPS mode enabled and an AD domain.

(BZ#1924707)

FreeRADIUS server fails to run in FIPS mode

By default, in FIPS mode, OpenSSL disables the use of the MD5 digest algorithm. As the RADIUS protocol requires MD5 to encrypt a secret between the RADIUS client and the RADIUS server, this causes the FreeRADIUS server to fail in FIPS mode.

To work around this problem, follow these steps:

Procedure

1. Create the environment variable, **RADIUS_MD5_FIPS_OVERRIDE** for the **radiusd** service:

```
systemctl edit radiusd

[Service]
Environment=RADIUS_MD5_FIPS_OVERRIDE=1
```

2. To apply the change, reload the **systemd** configuration and start the **radiusd** service:

```
# systemctl daemon-reload
# systemctl start radiusd
```

3. To run FreeRADIUS in debug mode:

```
# RADIUS_MD5_FIPS_OVERRIDE=1 radiusd -X
```

Note that though FreeRADIUS can run in FIPS mode, this does not mean that it is FIPS compliant as it uses weak ciphers and functions when in FIPS mode.

(BZ#1958979)

Actions required when running Samba as a print server

With this update, the **samba** package no longer creates the **/var/spool/samba/** directory. If you use Samba as a print server and use **/var/spool/samba/** in the **[printers]** share to spool print jobs, SELinux prevents Samba users from creating files in this directory. Consequently, print jobs fail and the **auditd** service logs a **denied** message in **/var/log/audit/audit.log**. To avoid this problem after updating your system to RHEL 8.5:

1. Search the **[printers]** share in the **/etc/samba/smb.conf** file.
2. If the share definition contains **path = /var/spool/samba/**, update the setting and set the **path** parameter to **/var/tmp/**.
3. Restart the **smbd** service:

```
# systemctl restart smbd
```

If you newly installed Samba on RHEL 8.5, no action is required. The default **/etc/samba/smb.conf** file provided by the **samba-common** package on RHEL 8.5 already uses the **/var/tmp/** directory to spool print jobs.

(BZ#2009213)

8.12. DESKTOP

Disabling flatpak repositories from Software Repositories is not possible

Currently, it is not possible to disable or remove **flatpak** repositories in the Software Repositories tool in the GNOME Software utility.

(BZ#1668760)

Drag-and-drop does not work between desktop and applications

Due to a bug in the **gnome-shell-extensions** package, the drag-and-drop functionality does not currently work between desktop and applications. Support for this feature will be added back in a future release.

(BZ#1717947)

Generation 2 RHEL 8 virtual machines sometimes fail to boot on Hyper-V Server 2016 hosts

When using RHEL 8 as the guest operating system on a virtual machine (VM) running on a Microsoft Hyper-V Server 2016 host, the VM in some cases fails to boot and returns to the GRUB boot menu. In addition, the following error is logged in the Hyper-V event log:

```
The guest operating system reported that it failed with the following error code: 0x1E
```

This error occurs due to a UEFI firmware bug on the Hyper-V host. To work around this problem, use Hyper-V Server 2019 as the host.

(BZ#1583445)

8.13. GRAPHICS INFRASTRUCTURES

Multiple HDR displays on a single MST topology may not power on

On systems using NVIDIA Turing GPUs with the **nouveau** driver, using a **DisplayPort** hub (such as a laptop dock) with multiple monitors which support HDR plugged into it may result in failure to turn on. This is due to the system erroneously thinking there is not enough bandwidth on the hub to support all of the displays.

(BZ#1812577)

radeon fails to reset hardware correctly

The **radeon** kernel driver currently does not reset hardware in the kexec context correctly. Instead, **radeon** falls over, which causes the rest of the **kdump** service to fail.

To work around this problem, disable **radeon** in **kdump** by adding the following line to the **/etc/kdump.conf** file:

```
dracut_args --omit-drivers "radeon"
force_rebuild 1
```

Restart the machine and **kdump**. After starting **kdump**, the **force_rebuild 1** line may be removed from the configuration file.

Note that in this scenario, no graphics will be available during **kdump**, but **kdump** will work successfully.

(BZ#1694705)

GUI in ESXi might crash due to low video memory

The graphical user interface (GUI) on RHEL virtual machines (VMs) in the VMware ESXi 7.0.1 hypervisor with vCenter Server 7.0.1 requires a certain amount of video memory. If you connect multiple consoles or high-resolution monitors to the VM, the GUI requires least 16 MB of video memory. If you start the GUI with less video memory, the GUI might terminate unexpectedly.

To work around the problem, configure the hypervisor to assign at least 16 MB of video memory to the VM. As a result, the GUI on the VM no longer crashes.

(BZ#1910358)

VNC Viewer displays wrong colors with the 16-bit color depth on IBM Z

The VNC Viewer application displays wrong colors when you connect to a VNC session on an IBM Z server with the 16-bit color depth.

To work around the problem, set the 24-bit color depth on the VNC server. With the **Xvnc** server, replace the **-depth 16** option with **-depth 24** in the **Xvnc** configuration.

As a result, VNC clients display the correct colors but use more network bandwidth with the server.

(BZ#1886147)

Matrox GPU with a VGA display shows no output

Your display might show no graphical output if you use the following system configuration:

- A GPU in the Matrox MGA G200 family
- A display connected over the VGA controller
- UEFI switched to legacy mode

As a consequence, you cannot use or install RHEL on this configuration.

To work around the problem, use the following procedure:

1. Boot the system to the boot loader menu.

2. Add the **nomodeset** option to the kernel command line.

As a result, RHEL boots and shows graphical output as expected, but the maximum resolution is limited.

(BZ#1953926)

Unable to run graphical applications using **sudo** command

When trying to run graphical applications as a user with elevated privileges, the application fails to open with an error message. The failure happens because **Xwayland** is restricted by the **Xauthority** file to use regular user credentials for authentication.

To work around this problem, use the **sudo -E** command to run graphical applications as a **root** user.

(BZ#1673073)

Hardware acceleration is not supported on ARM

Built-in graphics drivers do not support hardware acceleration or the Vulkan API on the 64-bit ARM architecture.

To enable hardware acceleration or Vulkan on ARM, install the proprietary Nvidia driver.

(JIRA:RHELPLAN-57914)

8.14. VIRTUALIZATION

Hot unplugging an IBMVFC device on PowerVM fails

When using a virtual machine (VM) with a RHEL 8 guest operating system on the PowerVM hypervisor, attempting to remove an IBM Power Virtual Fibre Channel (IBMVFC) device from the running VM currently fails. Instead, it displays an **outstanding translation** error.

To work around this problem, remove the IBMVFC device when the VM is shut down.

(BZ#1959020)

SMT CPU topology is not detected by VMs when using host passthrough mode on AMD EPYC

When a virtual machine (VM) boots with the CPU host passthrough mode on an AMD EPYC host, the **TOPOEXT** CPU feature flag is not present. Consequently, the VM is not able to detect a virtual CPU topology with multiple threads per core. To work around this problem, boot the VM with the EPYC CPU model instead of host passthrough.

(BZ#1740002)

IBM POWER hosts may crash when using the **ibmvfc** driver

When running RHEL 8 as a KVM virtualization host on a PowerVM logical partition (LPAR), a variety of errors may currently occur due problems with the **ibmvfc** driver. As a consequence, the host's kernel may panic under certain circumstances, such as:

- Using the Live Partition Mobility (LPM) feature
- Resetting a host adapter
- Using SCSI error handling (SCSI EH) functions

(BZ#1961722)

Using **perf kvm record** on IBM POWER Systems can cause the VM to crash

When using a RHEL 8 host on the little-endian variant of IBM POWER hardware, using the **perf kvm record** command to collect trace event samples for a KVM virtual machine (VM) in some cases results in the VM becoming unresponsive. This situation occurs when:

- The **perf** utility is used by an unprivileged user, and the **-p** option is used to identify the VM - for example **perf kvm record -e trace_cycles -p 12345**.
- The VM was started using the **virsh** shell.

To work around this problem, use the **perf kvm** utility with the **-i** option to monitor VMs that were created using the **virsh** shell. For example:

```
# perf kvm record -e trace_imc/trace_cycles/  -p <guest pid> -i
```

Note that when using the **-i** option, child tasks do not inherit counters, and threads will therefore not be monitored.

(BZ#1924016)

Attaching LUN devices to virtual machines using virtio-blk does not work

The q35 machine type does not support transitional virtio 1.0 devices, and RHEL 8 therefore lacks support for features that were deprecated in virtio 1.0. In particular, it is not possible on a RHEL 8 host to send SCSI commands from virtio-blk devices. As a consequence, attaching a physical disk as a LUN device to a virtual machine fails when using the virtio-blk controller.

Note that physical disks can still be passed through to the guest operating system, but they should be configured with the **device='disk'** option rather than **device='lun'**.

(BZ#1777138)

virsh iface-* commands do not work consistently

Currently, **virsh iface-*** commands, such as **virsh iface-start** and **virsh iface-destroy**, frequently fail due to configuration dependencies. Therefore, it is recommended not to use **virsh iface-*** commands for configuring and managing host network connections. Instead, use the NetworkManager program and its related management applications.

(BZ#1664592)

Virtual machines sometimes fail to start when using many virtio-blk disks

Adding a large number of virtio-blk devices to a virtual machine (VM) may exhaust the number of interrupt vectors available in the platform. If this occurs, the VM's guest OS fails to boot, and displays a **dracut-initqueue[392]: Warning: Could not boot** error.

(BZ#1719687)

Virtual machines with **iommu_platform=on** fail to start on IBM POWER

RHEL 8 currently does not support the **iommu_platform=on** parameter for virtual machines (VMs) on IBM POWER system. As a consequence, starting a VM with this parameter on IBM POWER hardware results in the VM becoming unresponsive during the boot process.

(BZ#1910848)

Windows Server 2016 virtual machines with Hyper-V enabled fail to boot when using certain CPU models

Currently, it is not possible to boot a virtual machine (VM) that uses Windows Server 2016 as the guest operating system, has the Hyper-V role enabled, and uses one of the following CPU models:

- EPYC-IBPB
- EPYC

To work around this problem, use the **EPYC-v3** CPU model, or manually enable the **xsaves** CPU flag for the VM.

(BZ#1942888)

Migrating a POWER9 guest from a RHEL 7-ALT host to RHEL 8 fails

Currently, migrating a POWER9 virtual machine from a RHEL 7-ALT host system to RHEL 8 becomes unresponsive with a **Migration status: active** status.

To work around this problem, disable Transparent Huge Pages (THP) on the RHEL 7-ALT host, which enables the migration to complete successfully.

(BZ#1741436)

Using **virt-customize** sometimes causes **guestfs-firstboot** to fail

After modifying a virtual machine (VM) disk image using the **virt-customize** utility, the **guestfs-firstboot** service in some cases fails due to incorrect SELinux permissions. This causes a variety of problems during VM startup, such as failing user creation or system registration.

To avoid this issue, add **--selinux-relabel** to the kernel command line of the VM after modifying its disk image with **virt-customize**.

(BZ#1554735)

Deleting a forward interface from a macvtap virtual network resets all connection counts of this network

Currently, deleting a forward interface from a **macvtap** virtual network with multiple forward interfaces also resets the connection status of the other forward interfaces of the network. As a consequence, the connection information in the live network XML is incorrect. Note, however, that this does not affect the functionality of the virtual network. To work around the issue, restart the **libvirtd** service on your host.

(BZ#1332758)

Virtual machines with SLOF fail to boot in netcat interfaces

When using a netcat (**nc**) interface to access the console of a virtual machine (VM) that is currently waiting at the Slimline Open Firmware (SLOF) prompt, the user input is ignored and VM stays unresponsive. To work around this problem, use the **nc -C** option when connecting to the VM, or use a telnet interface instead.

(BZ#1974622)

Mounting virtiofs directories fails in certain circumstances on RHEL 8 guests

Currently, when using the **virtiofs** feature to provide a host directory to a virtual machine (VM), mounting the directory on the VM fails with an "Operation not supported" error if the VM is using a RHEL 8.4 kernel but a RHEL 8.5 **selinux-policy** package.

To work around this issue, reboot the guest and boot it into the latest available kernel on the guest.

(BZ#1995558)

8.15. RHEL IN CLOUD ENVIRONMENTS

Setting static IP in a RHEL 8 virtual machine on a VMWare host does not work

Currently, when using RHEL 8 as a guest operating system of a virtual machine (VM) on a VMWare host, the DatasourceOVF function does not work correctly. As a consequence, if you use the **cloud-init** utility to set the VM's network to static IP and then reboot the VM, the VM's network will be changed to DHCP.

(BZ#1750862)

kdump sometimes does not start on Azure and Hyper-V

On RHEL 8 guest operating systems hosted on the Microsoft Azure or Hyper-V hypervisors, starting the **kdump** kernel in some cases fails when post-exec notifiers are enabled.

To work around this problem, disable crash kexec post notifiers:

```
# echo N > /sys/module/kernel/parameters/crash_kexec_post_notifiers
```

(BZ#1865745)

The SCSI host address sometimes changes when booting a Hyper-V VM with multiple guest disks

Currently, when booting a RHEL 8 virtual machine (VM) on the Hyper-V hypervisor, the host portion of the *Host, Bus, Target, Lun* (HBTL) SCSI address in some cases changes. As a consequence, automated tasks set up with the HBTL SCSI identification or device node in the VM do not work consistently. This occurs if the VM has more than one disk or if the disks have different sizes.

To work around the problem, modify your kickstart files, using one of the following methods:

Method 1: Use persistent identifiers for SCSI devices.

You can use for example the following powershell script to determine the specific device identifiers:

```
# Output what the /dev/disk/by-id/<value> for the specified hyper-v virtual disk.
# Takes a single parameter which is the virtual disk file.
# Note: kickstart syntax works with and without the /dev/ prefix.
param (
    [Parameter(Mandatory=$true)][string]$virtualdisk
)

$what = Get-VHD -Path $virtualdisk
$part = $what.DiskIdentifier.ToLower().split('-')

$p = $part[0]
$s0 = $p[6] + $p[7] + $p[4] + $p[5] + $p[2] + $p[3] + $p[0] + $p[1]
```

```
$p = $part[1]
$s1 =  $p[2] + $p[3] + $p[0] + $p[1]

[string]::format("/dev/disk/by-id/wwn-0x60022480{0}{1}{2}", $s0, $s1, $part[4])
```

You can use this script on the hyper-v host, for example as follows:

```
PS C:\Users\Public\Documents\Hyper-V\Virtual hard disks> .\by-id.ps1 .\Testing_8\disk_3_8.vhdx
/dev/disk/by-id/wwn-0x60022480e00bc367d7fd902e8bf0d3b4
PS C:\Users\Public\Documents\Hyper-V\Virtual hard disks> .\by-id.ps1 .\Testing_8\disk_3_9.vhdx
/dev/disk/by-id/wwn-0x600224807270e09717645b1890f8a9a2
```

Afterwards, the disk values can be used in the kickstart file, for example as follows:

```
part / --fstype=xfs --grow --asprimary --size=8192 --ondisk=/dev/disk/by-id/wwn-
0x600224807270e09717645b1890f8a9a2
part /home --fstype="xfs" --grow --ondisk=/dev/disk/by-id/wwn-
0x60022480e00bc367d7fd902e8bf0d3b4
```

As these values are specific for each virtual disk, the configuration needs to be done for each VM instance. It may, therefore, be useful to use the **%include** syntax to place the disk information into a separate file.

Method 2: Set up device selection by size.

A kickstart file that configures disk selection based on size must include lines similar to the following:

```
...

# Disk partitioning information is supplied in a file to kick start
%include /tmp/disks

...

# Partition information is created during install using the %pre section
%pre --interpreter /bin/bash --log /tmp/ks_pre.log

 # Dump whole SCSI/IDE disks out sorted from smallest to largest ouputting
 # just the name
 disks=(`lsblk -n -o NAME -l -b -x SIZE -d -I 8,3`) || exit 1

 # We are assuming we have 3 disks which will be used
 # and we will create some variables to represent
 d0=${disks[0]}
 d1=${disks[1]}
 d2=${disks[2]}

 echo "part /home --fstype="xfs" --ondisk=$d2 --grow" >> /tmp/disks
 echo "part swap --fstype="swap" --ondisk=$d0 --size=4096" >> /tmp/disks
 echo "part / --fstype="xfs" --ondisk=$d1 --grow" >> /tmp/disks
 echo "part /boot --fstype="xfs" --ondisk=$d1 --size=1024" >> /tmp/disks

%end
```

(BZ#1906870)

Hibernating RHEL 8 guests fails when FIPS mode is enabled

Currently, it is not possible to hibernate a virtual machine (VM) that uses RHEL 8 as its guest operating system if the VM is using FIPS mode.

(BZ#1934033, BZ#1944636)

8.16. SUPPORTABILITY

redhat-support-tool does not work with the **FUTURE** crypto policy

Because a cryptographic key used by a certificate on the Customer Portal API does not meet the requirements by the **FUTURE** system-wide cryptographic policy, the **redhat-support-tool** utility does not work with this policy level at the moment.

To work around this problem, use the **DEFAULT** crypto policy while connecting to the Customer Portal API.

(BZ#1802026)

CHAPTER 9. INTERNATIONALIZATION

9.1. RED HAT ENTERPRISE LINUX 8 INTERNATIONAL LANGUAGES

Red Hat Enterprise Linux 8 supports the installation of multiple languages and the changing of languages based on your requirements.

- East Asian Languages - Japanese, Korean, Simplified Chinese, and Traditional Chinese.
- European Languages - English, German, Spanish, French, Italian, Portuguese, and Russian.

The following table lists the fonts and input methods provided for various major languages.

Language	Default Font (Font Package)	Input Methods
English	dejavu-sans-fonts	
French	dejavu-sans-fonts	
German	dejavu-sans-fonts	
Italian	dejavu-sans-fonts	
Russian	dejavu-sans-fonts	
Spanish	dejavu-sans-fonts	
Portuguese	dejavu-sans-fonts	
Simplified Chinese	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-libpinyin, libpinyin
Traditional Chinese	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-libzhuyin, libzhuyin
Japanese	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-kkc, libkkc
Korean	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-hangul, libhangul

9.2. NOTABLE CHANGES TO INTERNATIONALIZATION IN RHEL 8

RHEL 8 introduces the following changes to internationalization compared to RHEL 7:

- Support for the **Unicode 11** computing industry standard has been added.
- Internationalization is distributed in multiple packages, which allows for smaller footprint installations. For more information, see Using langpacks.

- A number of **glibc** locales have been synchronized with Unicode Common Locale Data Repository (CLDR).

APPENDIX A. LIST OF TICKETS BY COMPONENT

Bugzilla and JIRA IDs are listed in this document for reference. Bugzilla bugs that are publicly accessible include a link to the ticket.

Component	Tickets
389-ds-base	BZ#1898541, BZ#1951020, BZ#1951020, BZ#1938239, BZ#1947044, BZ#1626633, BZ#1812286, BZ#1850664, BZ#1944494, BZ#1951020, BZ#1951020
NetworkManager	BZ#1912236, BZ#1899372, BZ#1942331, BZ#1934465, BZ#1548825, BZ#1920398
SLOF	BZ#1910848
accel-config	BZ#1843266
accountsservice	BZ#1812788
anaconda	BZ#1914955, BZ#1931069, BZ#1903786, BZ#1954408, BZ#1821192, BZ#1822880, BZ#1897657
ansible-collection-redhat-rhel_mgmt	BZ#1843859
apr	BZ#1819607
chrony	BZ#1939295, BZ#1895003
cloud-init	BZ#1957532, BZ#1750862
cmake	BZ#1957947
cockpit	BZ#1666722
corosync-qdevice	BZ#1784200
crash	BZ#1906482
createrepo_c	BZ#1973588
crun	BZ#1841438
crypto-policies	BZ#1960266, BZ#1876846, BZ#1933016, BZ#1919155, BZ#1660839
distribution	BZ#1953991, BZ#1657927

Component	Tickets
dracut	BZ#1929201
dwz	BZ#1948709
edk2	BZ#1741615, BZ#1935497
elfutils	BZ#1933890
fence-agents	BZ#1775847
firewalld	BZ#1872702, BZ#1871860
freeradius	BZ#1954521, BZ#1723362, BZ#1958979
gcc-toolset-11	BZ#1953094
gcc	BZ#1974402, BZ#1946758
gdb	BZ#1854784, BZ#1853140
glibc	BZ#1934155, BZ#1912670, BZ#1930302
gnome-shell-extensions	BZ#1717947
gnome-shell	BZ#1935261, BZ#1651378
gnome-software	BZ#1668760
gnutls	BZ#1965445, BZ#1628553
go-toolset	BZ#1938071
golang	BZ#1979100, BZ#1972825
grafana-container	BZ#1971557
grafana-pcp	BZ#1921190
grafana	BZ#1921191
grub2	BZ#1583445
hwloc	BZ#1917560

Component	Tickets
ipa	BZ#1924707, BZ#1664719, BZ#1664718
ipmitool	BZ#1951480
kernel	BZ#1944639, BZ#1907271, BZ#1924230, BZ#1954024, BZ#1570255, BZ#1938339, BZ#1957820, BZ#1865745, BZ#1836058, BZ#1906870, BZ#1934033, BZ#1924016, BZ#1942888, BZ#1868526, BZ#1812577, BZ#1694705, BZ#1910358, BZ#1953926, BZ#1730502, BZ#1930576, BZ#1609288, BZ#1793389, BZ#1666538, BZ#1602962, BZ#1940674, BZ#1920086, BZ#1971506, BZ#1519039, BZ#1627455, BZ#1501618, BZ#1495358, BZ#1633143, BZ#1814836, BZ#1696451, BZ#1348508, BZ#1839311, BZ#1783396, JIRA:RHELPLAN-57712, BZ#1837187, BZ#1904496, BZ#1660337, BZ#1905243, BZ#1665295, BZ#1569610
kexec-tools	BZ#1854037, BZ#1931266, BZ#2004000
krb5	BZ#1877991
libcomps	BZ#1960616
libgnome-keyring	BZ#1607766
libguestfs	BZ#1554735
libmodulemd	BZ#1894573, BZ#1984402
librepo	BZ#1814383
libreswan	BZ#1934058, BZ#1934859, BZ#1989050
libselinux-python-2.8-module	BZ#1666328
libservicelog	BZ#1844430
libvirt	BZ#1664592, BZ#1332758, BZ#1528684
linuxptp	BZ#1895005
llvm-toolset	BZ#1927937
lsvpd	BZ#1844428
lvm2	BZ#1899214, BZ#1496229, BZ#1768536
mariadb-connector-odbc	BZ#1944692

Component	Tickets
mariadb	BZ#1944653, BZ#1942330
mesa	BZ#1886147
modulemd-tools	BZ#1924850
mutt	BZ#1912614
net-snmp	BZ#1919714
nfs-utils	BZ#1868087, BZ#1592011
nginx	BZ#1945671
nispor	BZ#1848817
nodejs-16-container	BZ#2001020
nss_nis	BZ#1803161
nss	BZ#1817533, BZ#1645153
opal-prd	BZ#1921665
opencryptoki	BZ#1919223
opencv	BZ#1886310
openmpi	BZ#1866402
opensc	BZ#1947025
openscap	BZ#1959570, BZ#1953092, BZ#1966612
openslp	BZ#1965649
openssl	BZ#1810911
osbuild-composer	BZ#1945238, BZ#1937854, BZ#1915351, BZ#1951964
oscap-anaconda-addon	BZ#1691305, BZ#1674001, BZ#1834716, BZ#1843932, BZ#1665082
pacemaker	BZ#1948620, BZ#1443666
papi	BZ#1908126

Component	Tickets
pcp-container	BZ#1974912
pcp	BZ#1922040, BZ#1879350
pcs	BZ#1839637, BZ#1872378, BZ#1909901, BZ#1885293, BZ#1290830, BZ#1619620, BZ#1847102, BZ#1851335
pg_repack	BZ#1967193
php	BZ#1944110
pki-core	BZ#1729215
podman	BZ#1932083
postfix	BZ#1711885
powertop	BZ#1834722
ppc64-diag	BZ#1779206
pykickstart	BZ#1637872
qatlib	BZ#1920237
qemu-kvm	BZ#1740002, BZ#1719687, BZ#1651994
quota	BZ#1945408
rear	BZ#1983013, BZ#1930662, BZ#1958247, BZ#1988493, BZ#1958222, BZ#1983003, BZ#1747468, BZ#1868421
redhat-release	BZ#1935177
redhat-support-tool	BZ#1802026
rhel-system-roles	BZ#1960375, BZ#1866544, BZ#1961858, BZ#1958963, BZ#1938014, BZ#1954747, BZ#1854187, BZ#1757869, BZ#1938016, BZ#1986463, BZ#1970664, BZ#1970642, BZ#1848683, BZ#1963283, BZ#1938020, BZ#1938023, BZ#1957849, BZ#1959649, BZ#1939711, BZ#1943679, BZ#1882475, BZ#1876315, BZ#1894642, BZ#1978726, BZ#1893743
rpm	BZ#1938928, BZ#1688849
rsyslog	BZ#1891458, BZ#1932795, BZ#1679512, JIRA:RHELPLAN-10431

Component	Tickets
rt-tests	BZ#1954387
ruby	BZ#1938942
rust-toolset	BZ#1945805
samba	BZ#1944657, BZ#2009213, JIRA:RHELPLAN-13195
scap-security-guide	BZ#1857179, BZ#1946252, BZ#1955373, BZ#1966577, BZ#1970137, BZ#1993056, BZ#1993197, BZ#1876483, BZ#1955183, BZ#1843913, BZ#1858866, BZ#1750755
selinux-policy	BZ#1994096, BZ#1461914
socat	BZ#1947338
sos	BZ#1928679
spice	BZ#1849563
squid	BZ#1964384
sssd	BZ#1737489, BZ#1879869, BZ#1947671
systemtap	BZ#1933889
tboot	BZ#1947839
tesseract	BZ#1826085
tss2	BZ#1822073
tuned	BZ#1951992
udftools	BZ#1882531
udica	BZ#1763210
usbguard	BZ#2000000
valgrind	BZ#1933891
vdo	BZ#1949163

Component	Tickets
wayland	BZ#1673073
xfsprogs	BZ#1949743
xorg-x11-server	BZ#1698565
other	BZ#2005277, BZ#1839151, JIRA:RHELPLAN-89566, JIRA:RHELPLAN-92473, BZ#1935686, BZ#1986007, BZ#2011448, JIRA:RHELPLAN-99040, JIRA:RHELPLAN-99049, JIRA:RHELPLAN-99043, JIRA:RHELPLAN-99044, JIRA:RHELPLAN-99148, JIRA:RHELPLAN-61867, BZ#2013853, BZ#1971061, BZ#1959020, BZ#1897383, BZ#1961722, BZ#1777138, BZ#1640697, BZ#1659609, BZ#1687900, BZ#1697896, BZ#1757877, BZ#1741436, JIRA:RHELPLAN-59111, JIRA:RHELPLAN-27987, JIRA:RHELPLAN-28940, JIRA:RHELPLAN-34199, JIRA:RHELPLAN-57914, BZ#1987087, BZ#1974622, BZ#1995558, BZ#1690207, JIRA:RHELPLAN-1212, BZ#1559616, BZ#1889737, BZ#1812552, JIRA:RHELPLAN-14047, BZ#1769727, JIRA:RHELPLAN-27394, JIRA:RHELPLAN-27737, JIRA:RHELPLAN-56659, BZ#1906489, BZ#1957316, BZ#1960043, JIRA:RHELPLAN-58596, BZ#1642765, JIRA:RHELPLAN-10304, BZ#1646541, BZ#1647725, BZ#1932222, BZ#1686057, BZ#1748980, BZ#1958250, JIRA:RHELPLAN-71200, BZ#1827628, JIRA:RHELPLAN-45858, BZ#1871025, BZ#1871953, BZ#1874892, BZ#1893767, BZ#1916296, BZ#1926114, BZ#1904251, BZ#2011208, JIRA:RHELPLAN-59825, BZ#1920624, JIRA:RHELPLAN-70700, BZ#1929173, BZ#2006665, JIRA:RHELPLAN-98983

APPENDIX B. REVISION HISTORY