Abstract

The release notes provide high-level coverage of the improvements and additions that have been implemented in Red Hat Enterprise Linux 8.1 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!  ................................................................. 4

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION  ................................................. 5

CHAPTER 1. OVERVIEW  ................................................................. 6
  Infrastructure services  6
  Security  6
  Dynamic programming languages, web and database servers  6
  Compiler toolsets  6
  Installer and image creation  7
  Desktop  7
  Additional resources  7
    Red Hat Customer Portal Labs  7

CHAPTER 2. ARCHITECTURES  ......................................................... 9

CHAPTER 3. DISTRIBUTION OF CONTENT IN RHEL 8  .................................................. 10
  3.1. INSTALLATION  10
  3.2. REPOSITORIES  10
  3.3. APPLICATION STREAMS  11

CHAPTER 4. NEW FEATURES  .......................................................... 12
  4.1. THE WEB CONSOLE  12
  4.2. INSTALLER AND IMAGE CREATION  13
  4.3. KERNEL  13
  4.4. INFRASTRUCTURE SERVICES  15
  4.5. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS  16
  4.6. DESKTOP  19
  4.7. GRAPHICS INFRASTRUCTURES  19
  4.8. HARDWARE ENABLEMENT  20
  4.9. IDENTITY MANAGEMENT  20
  4.10. COMPILERS AND DEVELOPMENT TOOLS  22
  4.11. FILE SYSTEMS AND STORAGE  24
  4.12. HIGH AVAILABILITY AND CLUSTERS  25
  4.13. NETWORKING  25
  4.14. SECURITY  25
  4.15. VIRTUALIZATION  28

CHAPTER 5. BUG FIXES  ............................................................... 29
  5.1. INSTALLER AND IMAGE CREATION  29
  5.2. KERNEL  30
  5.3. SHELLS AND COMMAND-LINE TOOLS  31
  5.4. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS  31
  5.5. GRAPHICS INFRASTRUCTURES  32
  5.6. IDENTITY MANAGEMENT  32
  5.7. COMPILERS AND DEVELOPMENT TOOLS  32
  5.8. FILE SYSTEMS AND STORAGE  33
  5.9. NETWORKING  33
  5.10. SECURITY  34
  5.11. VIRTUALIZATION  34

CHAPTER 6. TECHNOLOGY PREVIEWS  .............................................. 35
  6.1. KERNEL  35
6.2. GRAPHICS INFRASTRUCTURES
6.3. HARDWARE ENABLEMENT
6.4. IDENTITY MANAGEMENT
6.5. FILE SYSTEMS AND STORAGE
6.6. HIGH AVAILABILITY AND CLUSTERS
6.7. NETWORKING
6.8. VIRTUALIZATION

CHAPTER 7. DEPRECATED FUNCTIONALITY
7.1. INSTALLER AND IMAGE CREATION
7.2. SOFTWARE MANAGEMENT
7.3. HARDWARE ENABLEMENT
7.4. FILE SYSTEMS AND STORAGE
7.5. NETWORKING
7.6. SECURITY
7.7. VIRTUALIZATION
7.8. DEPRECATED PACKAGES

CHAPTER 8. KNOWN ISSUES
8.1. THE WEB CONSOLE
8.2. INSTALLER AND IMAGE CREATION
8.3. KERNEL
8.4. SOFTWARE MANAGEMENT
8.5. INFRASTRUCTURE SERVICES
8.6. SHELLS AND COMMAND-LINE TOOLS
8.7. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS
8.8. DESKTOP
8.9. HARDWARE ENABLEMENT
8.10. IDENTITY MANAGEMENT
8.11. FILE SYSTEMS AND STORAGE
8.12. NETWORKING
8.13. SECURITY
8.14. SUBSCRIPTION MANAGEMENT
8.15. VIRTUALIZATION

CHAPTER 9. NOTABLE CHANGES TO CONTAINERS

CHAPTER 10. INTERNATIONALIZATION
10.1. RED HAT ENTERPRISE LINUX 8 INTERNATIONAL LANGUAGES
10.2. NOTABLE CHANGES TO INTERNATIONALIZATION IN RHEL 8

APPENDIX A. LIST OF TICKETS BY COMPONENT
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

Infrastructure services
RHEL 8.1 introduces a new routing protocol stack, FRR, which replaces Quagga that was used on previous versions of RHEL. FRR provides TCP/IP-based routing services with support for multiple IPv4 and IPv6 routing protocols. See Section 4.4, “Infrastructure services” for details.

The Tuned system tuning tool has been rebased to version 2.12, which adds support for negation of CPU list.

For more information, see Section 4.4, “Infrastructure services”.

The chrony suite has been rebased to version 3.5, which adds support for more accurate synchronization of the system clock with hardware timestamping in RHEL 8.1 kernel.

See Section 4.4, “Infrastructure services” for details.

Security

- RHEL 8.1 introduces a new tool for generation SELinux policies for containers - udica. With udica, you can create a tailored security policy for better control of how a container accesses host system resources, such as storage, devices, and network. This enables you to harden your container deployments against security violations and it also simplifies achieving and maintaining regulatory compliance.

- A security compliance suite, OpenSCAP, now supports SCAP 1.3 data streams and provides improved reports.


Dynamic programming languages, web and database servers
Later versions of the following components are now available as new module streams:

- PHP 7.3
- Ruby 2.6
- Node.js 12
- nginx 1.16

See Section 4.5, “Dynamic programming languages, web and database servers” for details.

Compiler toolsets
RHEL 8.1 introduces a new compiler toolset, GCC Toolset 9, an Application Stream packaged as a Software Collection, which provides recent versions of development tools.

In addition, the following compiler toolsets have been upgraded:

- LLVM 8.0.0
- Rust Toolset 1.35
- Go Toolset 1.12.6

See Section 4.10, ”Compilers and development tools” for more information.
Installer and image creation
Users can now disable modules during a Kickstart installation.

See Section 4.2, “Installer and image creation” for further details.

Desktop
Workspace switcher in the GNOME Classic environment has been modified. The switcher is now located in the right part of the bottom bar, and it is designed as a horizontal strip of thumbnails. Switching between workspaces is possible by clicking on the required thumbnail. For more information, see Section 4.6, “Desktop”.

The Direct Rendering Manager (DRM) kernel graphics subsystem has been rebased to upstream Linux kernel version 5.1. This version provides a number of enhancements over the previous version, including support for new GPUs and APUs, and various driver updates. See Section 4.6, “Desktop” for further details.

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.

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

- Registration Assistant
- Kickstart Generator
- Product Life Cycle Checker
- Red Hat Product Certificates
- Red Hat Satellite Upgrade Helper
- Red Hat CVE Checker
- JVM Options Configuration Tool
- Load Balancer Configuration Tool
- Red Hat Code Browser
- Yum Repository Configuration Helper
CHAPTER 2. ARCHITECTURES

Red Hat Enterprise Linux 8.1 is distributed with the kernel version 4.18, which provides support for the following architectures:

- AMD and Intel 64-bit architectures
- The 64-bit ARM architecture
- IBM Power Systems, Little Endian
- 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. Content in AppStream is available in one of two formats - the familiar RPM format and an extension to the RPM format called modules. 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. 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, two streams (versions) of the PostgreSQL database server are available in the postgresql module: PostgreSQL 10 (the default stream) and PostgreSQL 9.6. 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.
CHAPTER 4. NEW FEATURES

This part describes new features and major enhancements introduced in Red Hat Enterprise Linux 8.1.

4.1. THE WEB CONSOLE

Enabling and disabling SMT

Simultaneous Multi-.Threading (SMT) configuration is now available in RHEL 8. Disabling SMT in the web console allows you to mitigate a class of CPU security vulnerabilities such as:

- Microarchitectural Data Sampling
- L1 Terminal Fault Attack

(BZ#1678956)

Adding a search box in the Services page

The Services page now has a search box for filtering services by:

- Name
- Description
- State

In addition, service states have been merged into one list. The switcher buttons at the top of the page have also been changed to tabs to improve user experience of the Services page.

(BZ#1657752)

Adding support for firewall zones

The firewall settings on the Networking page now supports:

- Adding and removing zones
- Adding or removing services to arbitrary zones and
- Configuring custom ports in addition to firewalld services.

(BZ#1678473)

Adding improvements to Virtual Machines configuration

With this update, the RHEL 8 web console includes a lot of improvements in the Virtual Machines page. You can now:

- Manage various types of storage pools
- Configure VM autostart
- Import existing qcow images
- Install VMs through PXE boot
- Change memory allocation
Pause/resume VMs
- Configure cache characteristics (directsync, writeback)
- Change the boot order

(BZ#1658847)

4.2. INSTALLER AND IMAGE CREATION

Modules can now be disabled during Kickstart installation

With this enhancement, users can now disable a module to prevent the installation of packages from the module. To disable a module during Kickstart installation, use the command:

```
module --name=foo --stream=bar --disable
```

(BZ#1655523)

Support for the repo.git section to blueprints is now available

A new repo.git blueprint section allows users to include extra files in their image build. The files must be hosted in git repository that is accessible from the lorax-composer build server.

(BZ#1709594)

Image Builder now supports image creation for more cloud providers

With this update, the Image Builder expanded the number of Cloud Providers that the Image Builder can create an image for. As a result, now you can create RHEL images that can be deployed also on Google Cloud and Alibaba Cloud as well as run the custom instances on these platforms.

(BZ#1689140)

4.3. KERNEL

Red Hat Enterprise Linux 8 now supports early kdump

The early kdump feature allows the crash kernel and initramfs to load early enough to capture the vmcore information even for early crashes.

For more details about early kdump, see the `/usr/share/doc/kexec-tools/early-kdump-howto.txt` file.

(BZ#1520209)

RHEL 8 now supports ipcmni_extend

A new kernel command line parameter ipcmni_extend has been added to Red Hat Enterprise Linux 8. The parameter extends a number of unique System V Inter-process Communication (IPC) identifiers from the current maximum of 32 KB (15 bits) up to 16 MB (24 bits). As a result, users whose applications produce a lot of shared memory segments are able to create a stronger IPC identifier without exceeding the 32 KB limit.

Note that in some cases using ipcmni_extend results in a small performance overhead and it should be used only if the applications need more than 32 KB of unique IPC identifier.

(BZ#1710480)
The persistent memory initialization code supports parallel initialization

The persistent memory initialization code enables parallel initialization on systems with multiple nodes of persistent memory. The parallel initialization greatly reduces the overall memory initialization time on systems with large amounts of persistent memory. As a result, these systems can now boot much faster.

(BZ#1634343)

TPM userspace tool has been updated to the last version

The tpm2-tools userspace tool has been updated to version 2.0. With this update, tpm2-tools is able to fix many defects.

(BZ#1664498)

The rngd daemon is now able to run with non-root privileges

The random number generator daemon (rngd) checks whether data supplied by the source of randomness is sufficiently random and then stores the data in the kernel's random-number entropy pool. With this update, rngd is able to run with non-root user privileges to enhance system security.

(BZ#1692435)

UBSan has been enabled in the debug kernel in RHEL 8

The Undefined Behavior Sanitizer (UBSan) utility exposes undefined behavior flaws in C code languages at runtime. This utility has now been enabled in the debug kernel because the compiler behavior was, in some cases, different than developers' expectations. Especially, in the case of compiler optimization, where subtle, obscure bugs would appear. As a result, running the debug kernel with UBSan enabled allows the system to easily detect such bugs.

(BZ#1571628)

The bpftrace language support has been added in RHEL 8

Red Hat Enterprise Linux 8 supports the bpftrace language. bpftrace is a high-level tracing language for the extended Berkeley Packet Filter (eBPF) feature and is used for very specific tracing tasks while being easy to use. As a result, the user is able to achieve the same outcome with one line in bpftrace compared to a page of code that mixes Python and C in the BPF Compiler Collection (BCC) library.

(BZ#1687802)

The fadump infrastructure now supports re-registering in RHEL 8

The support has been added for re-registering (unregistering and registering) of the firmware-assisted dump (fadump) infrastructure after any memory hot add/remove operation to update the crash memory ranges. The feature aims to prevent the system from potential racing issues during unregistering and registering fadump from userspace during udev events.

(BZ#1710288)

The determine_maximum_mpps.sh script has been introduced in RHEL for Real Time 8

The determine_maximum_mpps.sh script has been introduced to help use the queuelat test program. The script executes queuelat to determine the maximum packets per second a machine can handle.

(BZ#1686494)

kernel-rt source tree now matches the latest RHEL 8 tree
The kernel-rt sources have been upgraded to be based on the latest Red Hat Enterprise Linux kernel source tree, which provides a number of bug fixes and enhancements over the previous version.

(BZ#1678887)

The ssdd test has been added to RHEL for Real Time 8

The ssdd test has been added to enable stress testing of the tracing subsystem. The test runs multiple tracing threads to verify locking is correct within the tracing system.

(BZ#1666351)

4.4. INFRASTRUCTURE SERVICES

tuned rebased to version 2.12

The tuned packages have been upgraded to upstream version 2.12, which provides a number of bug fixes and enhancements over the previous version, notably:

- Handling of devices that have been removed and reattached has been fixed.
- Support for negation of CPU list has been added.
- Performance of runtime kernel parameter configuration has been improved by switching from the sysctl tool to a new implementation specific to Tuned.

(BZ#1685585)

chrony rebased to version 3.5

The chrony packages have been upgraded to upstream version 3.5, which provides a number of bug fixes and enhancements over the previous version, notably:

- Support for more accurate synchronization of the system clock with hardware timestamping in RHEL 8.1 kernel has been added.
- Hardware timestamping has received significant improvements.
- The range of available polling intervals has been extended.
- The filter option has been added to NTP sources.

(BZ#1685469)

New FRRouting routing protocol stack is available

With this update, Quagga has been replaced by Free Range Routing (FRRouting, or FRR), which is a new routing protocol stack. FRR is provided by the frr package available in the AppStream repository.

FRR provides TCP/IP-based routing services with support for multiple IPv4 and IPv6 routing protocols, such as BGP, IS-IS, OSPF, PIM, and RIP.

With FRR installed, the system can act as a dedicated router, which exchanges routing information with other routers in either internal or external network.

For more information, see Setting the routing protocols for your system.

(BZ#1657029)
GNU enscript now supports ISO-8859-15 encoding
With this update, support for ISO-8859-15 encoding has been added into the GNU enscript program.

(BZ#1664366)

Improved accuracy of measuring system clock offset in phc2sys
The phc2sys program from the linuxptp packages now supports a more accurate method for measuring the offset of the system clock.

(BZ#1677217)

ptp4l now supports team interfaces in active-backup mode
With this update, support for team interfaces in active-backup mode has been added into the PTP Boundary/Ordinary Clock (ptp4l).

(BZ#1685467)

4.5. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS

A new module stream: php:7.3
RHEL 8.1 introduces PHP 7.3, which provides a number of new features and enhancements. Notable changes include:

- Enhanced and more flexible heredoc and nowdoc syntaces
- The PCRE extension upgraded to PCRE2
- Improved multibyte string handling
- Support for LDAP controls
- Improved FastCGI Process Manager (FPM) logging
- Several deprecations and backward incompatible changes

For more information, see Migrating from PHP 7.2.x to PHP 7.3.x.

Note that the RHEL 8 version of PHP 7.3 does not support the Argon2 password hashing algorithm.

To install the php:7.3 stream, use:

```bash
# yum install @php:7.3
```

If you want to upgrade from the php:7.2 stream, see Switching to a later stream.

(BZ#1653109)

A new module stream: ruby:2.6
A new module stream, ruby:2.6, is now available. Ruby 2.6.3, included in RHEL 8.1, provides numerous new features, enhancements, bug and security fixes, and performance improvements over version 2.5 distributed in RHEL 8.0.
Notable enhancements include:

- Constant names are now allowed to begin with a non-ASCII capital letter.
- Support for an endless range has been added.
- A new `Binding#source_location` method has been provided.
- `$SAFE` is now a process global state and it can be set back to 0.

The following performance improvements have been implemented:

- The `Proc#call` and `block.call` processes have been optimized.
- A new garbage collector managed heap, Transient heap (`theap`), has been introduced.
- Native implementations of coroutines for individual architectures have been introduced.

In addition, **Ruby 2.5**, provided by the `ruby:2.5` stream, has been upgraded to version 2.5.5, which provides a number of bug and security fixes.

To install the `ruby:2.6` stream, use:

```
# yum install @ruby:2.6
```

If you want to upgrade from the `ruby:2.5` stream, see Switching to a later stream.

(BZ#1672575)

**A new module stream: nodejs:12**

RHEL 8.1 introduces **Node.js 12**, which provides a number of new features and enhancements over version 10. Notable changes include:

- The V8 engine upgraded to version 7.4
- Improved performance
- A new experimental diagnostic report feature
- Support for ECMAScript 2015 (ES6) modules and improved support of native modules
- Worker threads no longer require a flag

To install the `nodejs:12` stream, use:

```
# yum install @nodejs:12
```

If you want to upgrade from the `nodejs:10` stream, see Switching to a later stream.

(BZ#1685191)

**A new module stream: nginx:1.16**

The **nginx 1.16** web and proxy server, which provides a number of new features and enhancements over version 1.14, is now available. For example:
Numerous updates related to SSL (loading of SSL certificates and secret keys from variables, variable support in the `ssl_certificate` and `ssl_certificate_key` directives, a new `ssl_early_data` directive)

- New directives (keepalive-related directives, a new `random` directive)
- New parameters and improvements to existing directives (port ranges for the `listen` directive, a new `delay` parameter for the `limit_req` directive)
- A new `$upstream_bytes_sent` variable

Other notable changes include:

- In the `nginx:1.16` stream, the `nginx` package does not require the `nginx-all-modules` package, therefore `nginx` modules must be installed explicitly. When you install `nginx` as module, the `nginx-all-modules` package is installed as a part of the `common` profile, which is the default profile.

- The `ssl` directive has been deprecated; use the `ssl` parameter for the `listen` directive instead.

- `nginx` now detects missing SSL certificates during configuration testing.

- When using a host name in the `listen` directive, `nginx` now creates listening sockets for all addresses that the host name resolves to.

To install the `nginx:1.16` stream, use:

```
# yum install @nginx:1.16
```

If you want to upgrade from the `nginx:1.14` stream, see [Switching to a later stream](#).

(BZ#1690292)

perl-IO-Socket-SSL rebased to version 2.066

The `perl-IO-Socket-SSL` package has been upgraded to version 2.066, which provides a number of bug fixes and enhancements over the previous version, for example:

- Improved support for TLS 1.3, notably a session reuse and an automatic post-handshake authentication on the client side

- Added support for multiple curves, automatic setting of curves, partial trust chains, and support for RSA and ECDSA certificates on the same domain

(BZ#1632600)

perl-Net-SSLeay rebased to version 1.88

The `perl-Net-SSLeay` package has been upgraded to version 1.88, which provides multiple bug fixes and enhancements. Notable changes include:

- Improved compatibility with OpenSSL 1.1.1, such as manipulating a stack of certificates and X509 stores, and selecting elliptic curves and groups

- Improved compatibility with TLS 1.3, for example, a session reuse and a post-handshake authentication

- Fixed memory leak in the `cb_data_advanced_put()` subroutine.
4.6. DESKTOP

Modified workspace switcher in GNOME Classic

Workspace switcher in the GNOME Classic environment has been modified. The switcher is now located in the right part of the bottom bar, and it is designed as a horizontal strip of thumbnails. Switching between workspaces is possible by clicking on the required thumbnail. Alternatively, you can also use the combination of kbd:[Ctrl + Alt + down/up arrow] keys to switch between workspaces. The content of the active workspace is shown in the left part of the bottom bar in form of the window list.

When you press the kbd:[Super] key within the particular workspace, you can see the window picker, which includes all windows that are open in this workspace. However, the window picker no longer displays the following elements that were available in the previous release of RHEL:

- dock (vertical bar on the left side of the screen)
- workspace switcher (vertical bar on the right side of the screen)
- search entry

For particular tasks that were previously achieved with the help of these elements, adopt the following approaches:

- To launch applications, instead of using dock, you can:
  - Use the Applications menu on the top bar
  - Press the kbd:[Alt + F2] keys to make the Enter a Command screen appear, and write the name of the executable into this screen.

- To switch between workspaces, instead of using the vertical workspace switcher, use the horizontal workspace switcher in the right bottom bar.

- If you require the search entry or the vertical workspace switcher, use GNOME Standard environment instead of GNOME Classic.

4.7. GRAPHICS INFRASTRUCTURES

DRM rebased to Linux kernel version 5.1

The Direct Rendering Manager (DRM) kernel graphics subsystem has been rebased to upstream Linux kernel version 5.1, which provides a number of bug fixes and enhancements over the previous version. Most notably:

- The mgag200 driver has been updated. The driver continues providing support for HPE Proliant Gen10 Systems, which use Matrox G200 eH3 GPUs. The updated driver also supports current and new Dell EMC PowerEdge Servers.

- The nouveau driver has been updated to provide hardware enablement to current and future Lenovo platforms that use NVIDIA GPUs.

- The i915 display driver has been updated for continued support of current and new Intel GPUs.
- Bug fixes for Aspeed AST BMC display chips have been added.
- Support for AMD Raven 2 set of Accelerated Processing Units (APUs) has been added.
- Support for AMD Picasso APUs has been added.
- Support for AMD Vega GPUs has been added.
- Support for Intel Amber Lake-Y and Intel Comet Lake-U GPUs has been added.

(BZ#1685552)

4.8. HARDWARE ENABLEMENT

Memory Mode for Optane DC Persistent Memory technology is fully supported

Intel Optane DC Persistent Memory storage devices provide data center-class persistent memory technology, which can significantly increase transaction throughput.

To use the Memory Mode technology, your system does not require any special drivers or specific certification. Memory Mode is transparent to the operating system.

(BZ#1718422)

4.9. IDENTITY MANAGEMENT

Setting up IdM as a hidden replica is now available as a Technology Preview

This enhancement enables administrators to set up an Identity Management (IdM) replica as a hidden replica. A hidden replica is an IdM server that has all services running and available. However, it is not advertised to other clients or masters because no SRV records exist for the services in DNS, and LDAP server roles are not enabled. Therefore, clients cannot use service discovery to detect hidden replicas.

Hidden replicas are primarily designed for dedicated services that can otherwise disrupt clients. For example, a full backup of IdM requires to shut down all IdM services on the master or replica. Since no clients use a hidden replica, administrators can temporarily shut down the services on this host without affecting any clients. Other use cases include high-load operations on the IdM API or the LDAP server, such as a mass import or extensive queries.

To install a new hidden replica, use the `ipa-replica-install --hidden-replica` command. To change the state of an existing replica, use the `ipa server-state` command.

(BZ#1719767)

Identity Management supports trust with Windows Server 2019

When using Identity Management, you can now establish a supported forest trust to Active Directory forests that run by Windows Server 2019. The supported forest and domain functional levels are unchanged and supported up to level Windows Server 2016.

(JIRA:RHELPLAN-15036)

IdM now supports renewing expired system certificates when the server is offline

With this enhancement, administrators can renew expired system certificates when Identity Management (IdM) is offline. When a system certificate expires, IdM fails to start. The new `ipa-cert-fix` command replaces the workaround to manually set the date back to proceed with the renewal process.
As a result, the downtime and support costs reduce in the mentioned scenario.

(JIRA:RHELPLAN-13074)

**New ipa-crl-generation commands have been introduced to simplify managing IdM CRL master**

This update introduces the `ipa-crl-generation status/enable/disable` commands. These commands, run by the root user, simplify work with the Certificate Revocation List (CRL) in IdM. Previously, moving the CRL generation master from one IdM CA server to another was a lengthy, manual and error-prone procedure.

The `ipa-crl-generation status` command checks if the current host is the CRL generation master. The `ipa-crl-generation enable` command makes the current host the CRL generation master in IdM if the current host is an IdM CA server. The `ipa-crl-generation disable` command stops CRL generation on the current host.

Additionally, the `ipa-server-install --uninstall` command now includes a safeguard checking whether the host is the CRL generation master. This way, IdM ensures that the system administrator does not remove the CRL generation master from the topology.

(JIRA:RHELPLAN-13068)

**New tool to test the overall fitness of IdM deployment: Healthcheck**

This update introduces the **Healthcheck** tool in Identity Management (IdM). The tool provides tests verifying that the current IdM server is configured and running correctly.

The major areas currently covered are: * Certificate configuration and expiration dates * Replication errors * Replication topology * AD Trust configuration * Service status * File permissions of important configuration files * Filesystem space

The **Healthcheck** tool is available in the command-line interface (CLI).

(JIRA:RHELPLAN-13066)

**OpenID Connect support in keycloak-httpd-client-install**

The `keycloak-httpd-client-install` identity provider previously supported only the SAML (Security Assertion Markup Language) authentication with the `mod_auth_mellon` authentication module. This rebase brings the `mod_auth_openidc` authentication module support, which allows you to configure also the OpenID Connect authentication.

The `keycloak-httpd-client-install` identity provider allows an apache instance to be configured as an OpenID Connect client by configuring `mod_auth_openidc`.

(BZ#1553890)

**IdM now supports Ansible roles and modules for installation and management**

This update introduces the **ansible-freeipa** package, which provides Ansible roles and modules for Identity Management (IdM) deployment and management. You can use Ansible roles to install and uninstall IdM servers, replicas, and clients. You can use Ansible modules to manage IdM groups, topology, and users. There are also example playbooks available.

This update simplifies the installation and configuration of IdM based solutions.

(JIRA:RHELPLAN-2542)
4.10. COMPILERS AND DEVELOPMENT TOOLS

GCC Toolset 9 available

Red Hat Enterprise Linux 8.1 introduces GCC Toolset 9, an Application Stream containing more up-to-date versions of development tools.

The following tools and versions are provided by GCC Toolset 9:

<table>
<thead>
<tr>
<th>Tool</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>GCC</td>
<td>9.1.1</td>
</tr>
<tr>
<td>GDB</td>
<td>8.3</td>
</tr>
<tr>
<td>Valgrind</td>
<td>3.15.0</td>
</tr>
<tr>
<td>SystemTap</td>
<td>4.1</td>
</tr>
<tr>
<td>Dyninst</td>
<td>10.1.0</td>
</tr>
<tr>
<td>binutils</td>
<td>2.32</td>
</tr>
<tr>
<td>elfutils</td>
<td>0.176</td>
</tr>
<tr>
<td>dwz</td>
<td>0.12</td>
</tr>
<tr>
<td>make</td>
<td>4.2.1</td>
</tr>
<tr>
<td>strace</td>
<td>5.1</td>
</tr>
<tr>
<td>ltrace</td>
<td>0.7.91</td>
</tr>
</tbody>
</table>

GCC Toolset 9 is available as an Application Stream in the form of a Software Collection in the AppStream repository. GCC Toolset is a set of tools similar to Red Hat Developer Toolset for RHEL 7.

To install GCC Toolset 9:

```
# yum install gcc-toolset-9
```

To run a tool from GCC Toolset 9:

```
$ scl enable gcc-toolset-9 tool
```

To run a shell session where tool versions from GCC Toolset 9 take precedence over system versions of these tools:

```
$ scl enable gcc-toolset-9 bash
```

(BZ#1685482)
Upgraded compiler toolsets

The following compiler toolsets, distributed as Application Streams, have been upgraded with RHEL 8.1 Beta:

- Clang and LLVM Toolset, which provides the LLVM compiler infrastructure framework, the Clang compiler for the C and C++ languages, the LLDB debugger, and related tools for code analysis, to version 8.0.0
- Rust Toolset, which provides the Rust programming language compiler rustc, the cargo build tool and dependency manager, and required libraries, to version 1.35
- Go Toolset, which provides the Go (golang) programming language tools and libraries, to version 1.12.6.

(BZ#1731502, BZ#1691975, BZ#1680091, BZ#1677819, BZ#1681643)

SystemTap rebased to version 4.1

The SystemTap instrumentation tool has been updated to upstream version 4.1. Notable improvements include:

- The eBPF runtime backend can handle more features of the scripting language such as string variables and rich formatted printing.
- Performance of the translator has been significantly improved.
- More types of data in optimized C code can now be extracted with DWARF4 debuginfo constructs.

(BZ#1675740)

efuse ls rebased to version 0.176

The elfutils packages have been updated to upstream version 0.176. This version brings various bug fixes, and resolves the following vulnerabilities:

- CVE-2019-7146
- CVE-2019-7149
- CVE-2019-7150
- CVE-2019-7664
- CVE-2019-7665

Notable improvements include:

- The libdw library has been extended with the dwelf_elf_begin() function which is a variant of elf_begin() that handles compressed files.
- A new --reloc-debug-sections-only option has been added to the eu-strip tool to resolve all trivial relocations between debug sections in place without any other stripping. This functionality is relevant only for ET_REL files in certain circumstances.

(BZ#1683705)

Date formatting updates for the Japanese Reiwa era
The GNU C Library now provides correct Japanese era name formatting for the Reiwa era starting on May 1st, 2019. The time handling API data has been updated, including the data used by the \texttt{strftime} and \texttt{strptime} functions. All APIs will correctly print the Reiwa era including when \texttt{strftime} is used along with one of the era conversion specifiers such as \texttt{%EC}, \texttt{%EY}, or \texttt{%Ey}.

(BZ\#1577438)

4.11. FILE SYSTEMS AND STORAGE

Support for Data Integrity Field/Data Integrity Extension (DIF/DIX)

DIF/DIX is supported on configurations where the hardware vendor has qualified it and provides full support for the particular host bus adapter (HBA) and storage array configuration on RHEL.

DIF/DIX is not supported on the following configurations:

- It is not supported for use on the boot device.
- It is not supported on virtualized guests.
- Red Hat does not support using the Automatic Storage Management library (ASMLib) when DIF/DIX is enabled.

DIF/DIX is enabled or disabled at the storage device, which involves various layers up to (and including) the application. The method for activating the DIF on storage devices is device-dependent.

For further information on the DIF/DIX feature, see What is DIF/DIX.

(BZ\#1649493)

Optane DC memory systems now supports EDAC reports

Previously, EDAC was not reporting memory corrected/uncorrected events if the memory address was within a NVDIMM module. With this update, EDAC can properly report the events with the correct memory module information.

(BZ\#1571534)

The VDO Ansible module has been moved to Ansible packages

Previously, the VDO Ansible module was provided by the \texttt{vdo} RPM package. Starting with this release, the module is provided by the \texttt{ansible} package instead.

The original location of the VDO Ansible module file was:

```
/usr/share/doc/vdo/examples/ansible/vdo.py
```

The new location of the file is:

```
/usr/lib/python3.6/site-packages/ansible/modules/system/vdo.py
```

The \texttt{vdo} package continues to distribute Ansible playbooks.

For more information on Ansible, see http://docs.ansible.com/.

(BZ\#1669534)
Aero adapters are now fully supported

The following Aero adapters, previously available as a Technology Preview, are now fully supported:

- PCI ID 0x1000:0x00e2 and 0x1000:0x00e6, controlled by the `mpt3sas` driver
- PCI ID 0x1000:0x10e5 and 0x1000:0x10e6, controlled by the `megaraid_sas` driver

(BZ#1663281)

4.12. HIGH AVAILABILITY AND CLUSTERS

Extending a shared logical volume no longer requires a refresh on every cluster node

With this release, extending a shared logical volume no longer requires a refresh on every cluster node after running the `lvextend` command on one cluster node. For the full procedure to extend the size of a GFS2 file system, see Growing a GFS2 file system.

(BZ#1649086)

Maximum size of a supported RHEL HA cluster increased from 16 to 32 nodes

With this release, Red Hat supports cluster deployments of up to 32 full cluster nodes.

(BZ#1693491)

4.13. NETWORKING

PMTU discovery and route redirection is now supported with VXLAN and GENEVE tunnels

Previously, the kernel in Red Hat Enterprise Linux (RHEL) did not handle Internet Control Message Protocol (ICMP) and ICMPv6 messages for Virtual Extensible LAN (VXLAN) and Generic Network Virtualization Encapsulation (GENEVE) tunnels. As a consequence, Path MTU (PMTU) discovery and route redirection was not supported with VXLAN and GENEVE tunnels. With this update, the kernel handles ICMP "Destination Unreachable" and "Redirect Message", as well as ICMPv6 "Packet Too Big" and "Destination Unreachable" error messages by adjusting the PMTU and modifying forwarding information. As a result, PMTU discovery and route redirection are now supported with VXLAN and GENEVE tunnels.

(BZ#1652222)

Notable changes in XDP and networking eBPF features in kernel

The XDP and the networking eBPF features in the kernel package have been upgraded to upstream version 5.0, which provides a number of bug fixes and enhancements over the previous version:

- eBPF programs can now better interact with the TCP/IP stack, perform flow dissection, have wider range of `bpf` helpers available, and have access to new map types.
- XDP metadata are now available to AF_XDP sockets.

(BZ#1687459)

4.14. SECURITY

SELinux user-space tools updated to version 2.9
The `libsepol`, `libselinux`, `libsemanage`, `policycoreutils`, `checkpolicy`, and `mcstrans` SELinux user-space tools have been upgraded to the latest upstream release 2.9, which provides many bug fixes and enhancements over the previous version.

(BZ#1672638, BZ#1672642, BZ#1672637, BZ#1672640, BZ#1672635, BZ#1672641)

**libssh now complies with the system-wide crypto-policies**

The `libssh` client and server now automatically load the `/etc/libssh/libssh_client.config` file and the `/etc/libssh/libssh_server.config`, respectively. This configuration file includes the options set by the system-wide `crypto-policies` component for the `libssh` back end and the options set in the `/etc/ssh/sshd_config` or `/etc/ssh/ssh_config` OpenSSH configuration file. With automatic loading of the configuration file, `libssh` now use the system-wide cryptographic settings set by `crypto-policies`. This change simplifies control over the set of used cryptographic algorithms by applications.

(BZ#1610883, BZ#1610884)

**SETools updated to version 4.2.2**

The SETools collection of tools and libraries has been upgraded to the latest upstream release 4.2.2, which provides the following changes:

- Removed source policy references from man pages, as loading source policies is no longer supported
- Fixed a performance regression in alias loading

(BZ#1672631)

**OpenSCAP rebased to version 1.3.1**

The `openscap` packages have been upgraded to upstream version 1.3.1, which provides many bug fixes and enhancements over the previous version, most notably:

- Support for SCAP 1.3 source data streams: evaluating, XML schemas, and validation
- Tailoring files are included in ARF result files
- OVAL details are always shown in HTML reports, users do not have to provide the `--oval-results` option
- HTML report displays OVAL test details also for OVAL tests included from other OVAL definitions using the OVAL `extend_definition` element
- OVAL test IDs are shown in HTML reports
- Rule IDs are shown in HTML guides

(BZ#1718826)

**scap-security-guide rebased to version 0.1.44**

The `scap-security-guide` packages have been upgraded to upstream version 0.1.44, which provides many bug fixes and enhancements over the previous version, most notably:

- SCAP content conforms to the latest version of SCAP standard, SCAP 1.3
- SCAP content supports UBI images

(BZ#1718839)

OpenSCAP now supports SCAP 1.3
The OpenSCAP suite now supports data streams conforming to the latest version of the SCAP standard - SCAP 1.3. You can now use SCAP 1.3 data streams, such as those contained in the scap-security-guide package, in the same way as SCAP 1.2 data streams without any additional usability restrictions.

(BZ#1709429)

OpenSSH rebased to 8.0p1

The openssh packages have been upgraded to upstream version 8.0p1, which provides many bug fixes and enhancements over the previous version, most notably:

- Increased default RSA key size to 3072 bits for the ssh-keygen tool
- Removed support for the ShowPatchLevel configuration option
- Applied numerous GSSAPI key exchange code fixes, such as the fix of Kerberos cleanup procedures
- Removed fall back to the sshd_net_t SELinux context
- Added support for Match final blocks
- Fixed minor issues in the ssh-copy-id command

(BZ#1691045)

A new SELinux policy class: bpf

A new SELinux policy class, bpf, has been introduced. The bpf class enables users to control the Berkeley Packet Filter (BPF) flow through SElinux, and allows inspection and simple manipulation of Extended Berkeley Packet Filter (eBPF) programs and maps controlled by SElinux.

(BZ#1673056)

A new SELinux type: boltd_t

A new SELinux type, boltd_t, confines boltd, a system daemon for managing Thunderbolt 3 devices. As a result, boltd now runs as a confined service in SELinux enforcing mode.

(BZ#1684103)

New package: udica

The new udica package provides a tool for generation SELinux policies for containers. With udica, you can create a tailored security policy for better control of how a container accesses host system resources, such as storage, devices, and network. This enables you to harden your container deployments against security violations and it also simplifies achieving and maintaining regulatory compliance.

(BZ#1673643)

selinux-policy rebased to 3.14.3

The selinux-policy package has been upgraded to upstream version 3.14.3, which provides a number of bug fixes and enhancements to the allow rules over the previous version.
4.15. VIRTUALIZATION

Windows automatically finds the needed virtio-win drivers

Windows can now automatically find the virtio-win drivers it needs from the driver ISO without requiring the user to select the folder in which they are located.

(BZ#1673107) (BZ#1223668)
CHAPTER 5. BUG FIXES

This part describes bugs fixed in Red Hat Enterprise Linux 8.1 that have a significant impact on users.

5.1. INSTALLER AND IMAGE CREATION

The `xorg-x11-drv-fbdev`, `xorg-x11-drv-vesa`, and `xorg-x11-drv-vmware` video drivers are now installed by default

Previously, workstations with specific models of NVIDIA graphics cards and workstations with specific AMD accelerated processing units did not display the graphical login window after a RHEL 8.0 Server installation. This issue also impacted virtual machines relying on EFI for graphics support, such as Hyper-V. With this update, the `xorg-x11-drv-fbdev`, `xorg-x11-drv-vesa`, and `xorg-x11-drv-vmware` video drivers are installed by default and the graphical login window is displayed after a RHEL 8.0 Server installation.

(BZ#1687489)

Rescue mode no longer fails without displaying an error message

Previously, running rescue mode on a system with no Linux partitions resulted in the installation program failing with an exception. With this update, the installation program displays the error message “You don’t have any Linux partitions” when a system with no Linux partitions is detected.

(BZ#1628653)

The installation program now sets the `lvm_metadata_backup` Blivet flag for image installations

Previously, the installation program failed to set the `lvm_metadata_backup` Blivet flag for image installations. As a consequence, LVM backup files were located in the `/etc/lvm/` subdirectory after an image installation. With this update, the installation program sets the `lvm_metadata_backup` Blivet flag, and as a result, there are no LVM backup files located in the `/etc/lvm/` subdirectory after an image installation.

(BZ#1673901)

The RHEL 8 installation program now uses the entry ID to set the default boot entry

Previously, the RHEL 8 installation program used the index of the first boot entry as the default, instead of using the entry ID. As a consequence, adding a new boot entry became the default, as it was sorted first and set to the first index. With this update, the installation program uses the entry ID to set the default boot entry, and as a result, the default entry is not changed, even if boot entries are added and sorted before the default.

(BZ#1671047)

The RHEL 8 installation program now handles strings from RPM

Previously, when the `python3-rpm` library returned a string, the installation program failed with an exception. With this update, the installation program can now handle strings from RPM.

(BZ#1689909)

The `inst.repo` kernel boot parameter now works for a repository on a hard drive that has a non-root path
Previously, the RHEL 8 installation process could not proceed without manual intervention if the `inst.repo=hd:<device>:<path>` kernel boot parameter was pointing to a repository (not an ISO image) on a hard drive, and a non-root (/) path was used. With this update, the installation program can now propagate any `<path>` for a repository located on a hard drive, ensuring the installation proceeds as normal.

(BZ#1689194)

The `--changesok` option now allows the installation program to change the root password

Previously, using the `--changesok` option when installing Red Hat Enterprise Linux 8 from a Kickstart file did not allow the installation program to change the root password. With this update, the `--changesok` option is successfully passed by Kickstart, and as a result, users specifying the `pwpolicy root --changesok` option in their Kickstart file can now change the root password using the GUI, even if the password has already been set by Kickstart.

(BZ#1584145)

Image Building no longer fails when using `lorax-composer API`

Previously, when using `lorax-composer` API from a subscribed RHEL system, the image building process always failed. Anaconda could not access the repositories, because the subscription certificates from the host are not passed through. To fix the issue update `lorax-composer`, `pykickstart`, and `Anaconda` packages. That will allow to pass supported CDN certificates.

(BZ#1663950)

5.2. KERNEL

tmp2-abrmd-selinux now has a proper dependency on `selinux-policy-targeted`

Previously, the `tpm2-abrmd-selinux` package had a dependency on the `selinux-policy-base` package instead of the `selinux-policy-targeted` package. Consequently, if a system had `selinux-policy-minimum` installed instead of `selinux-policy-targeted`, installation of the `tpm2-abrmd-selinux` package failed. This update fixes the bug and `tpm2-abrmd-selinux` can be installed correctly in the described scenario.

(BZ#1642000)

All `/sys/kernel/debug` files can be accessed

Previously, the return value for "Operation not permitted" (EPERM) error remained set until the end of the function regardless of the error. Consequently, any attempts to access certain `/sys/kernel/debug` (debugfs) files failed with an unwarranted EPERM error. This update moves the EPERM return value to the following block. As a result, `debugfs` files can be accessed without problems in the described scenario.

(BZ#1686755)

`podman` is able to checkpoint containers in RHEL 8

Previously, the version of the Checkpoint and Restore In Userspace (CRIU) package was outdated. Consequently, CRIU did not support container checkpoint and restore functionality, and the `podman` utility failed to checkpoint containers. When running the `podman container checkpoint` command, the following error message was displayed:

> 'checkpointing a container requires at least CRIU 31100'
This update fixes the problem by upgrading the version of the CRIU package. As a result, podman now supports container checkpoint and restore functionality.

(BZ#1689746)

**early-kdump and standard kdump no longer fail if the `add_dracutmodules+=earlykdump` option is used in dracut.conf**

Previously, an inconsistency occurred between the kernel version being installed for early-kdump and the kernel version initramfs was generated for. As a consequence, booting failed when early-kdump was enabled. In addition, if early-kdump detected that it was being included in a standard kdump initramfs image, it forced an exit. Therefore the standard kdump service also failed when trying to rebuild kdump initramfs if early-kdump was added as a default dracut module. As a consequence, early-kdump and standard kdump both failed. With this update, early-kdump uses the consistent kernel name during the installation, only the version differs from the running kernel. Also, the standard kdump service will forcibly drop early-kdump to avoid image generation failure. As a result, early-kdump and standard kdump no longer fail in the described scenario.

(BZ#1662911)

**The first kernel with SME enabled now succeeds in dumping the vmcore**

Previously, the encrypted memory in the first kernel with the active Secure Memory Encryption (SME) feature caused a failure of the kdump mechanism. Consequently, the first kernel was not able to dump the contents (vmcore) of its memory. With this update, the ioremap_encrypted() function has been added to remap the encrypted memory and modify the related code. As a result, the encrypted first kernel’s memory is now properly accessed, and the vmcore can be dumped and parsed by the crash tools in the described scenario.

(BZ#1564427)

**C-state transitions can now be disabled during hwlatdetect runs**

To achieve real-time performance, the hwlatdetect utility needs to be able to disable power saving in the CPU during test runs. This update allows hwlatdetect to turn off C-state transitions for the duration of the test run and hwlatdetect is now able to detect hardware latencies more accurately.

(BZ#1707505)

### 5.3. SHELLS AND COMMAND-LINE TOOLS

**systemd in debug mode no longer produces unnecessary log messages**

When using the systemd system and service manager in debug mode, systemd previously produced unnecessary and harmless log messages that started with:

```
"Failed to add rule for system call ..."
```

With this update, systemd has been fixed to no longer produce these unnecessary debug messages.

(BZ#1658691)

### 5.4. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS
Socket::inet_aton() can now be used from multiple threads safely

Previously, the Socket::inet_aton() function, used for resolving a domain name from multiple Perl threads, called the unsafe gethostbyname() glibc function. Consequently, an incorrect IPv4 address was occasionally returned, or the Perl interpreter terminated unexpectedly. With this update, the Socket::inet_aton() implementation has been changed to use the thread-safe getaddrinfo() glibc function instead of gethostbyname(). As a result, the inet_aton() function from Perl Socket module can be used from multiple threads safely.

(BZ#1699793, BZ#1699958)

5.5. GRAPHICS INFRASTRUCTURES

Error initializing the GPU driver when booting Linux guest

Previously, as GVT-g only simulates the DP port for guest and leaves the EDP_PSR_IMR and EDP_PSR_IIR registers as default MMIO read/write, when initializing the GPU driver, Linux guests emitted the warning: Interrupt register 0x64838 is not zero: 0xffffffff. To resolve this issue, handlers have been added to these registers and the warning is no longer returned.

(BZ#1643980)

5.6. IDENTITY MANAGEMENT

FreeRADIUS now resolves hostnames pointing to IPv6 addresses

In previous RHEL 8 versions of FreeRADIUS, the ipaddr utility only supported IPv4 addresses. Consequently, for the radiusd daemon to resolve IPv6 addresses, a manual update of the configuration was required after an upgrade of the system from RHEL 7 to RHEL 8. This update fixes the underlying code, and ipaddr in FreeRADIUS now uses IPv6 addresses, too.

(BZ#1685546)

The Nuxwdog service no longer fails to start the PKI server in HSM environments

Previously, due to bugs, the keyutils package was not installed as a dependency of the pki-core package. Additionally, the Nuxwdog watchdog service failed to start the public key infrastructure (PKI) server in environments that use a hardware security module (HSM). These problems have been fixed. As a result, the required keyutils package is now installed automatically as a dependency, and Nuxwdog starts the PKI server as expected in environments with HSM.

(BZ#1695302)

Samba no longer denies access when using the sss ID mapping plug-in

Previously, when you ran Samba on the domain member with this configuration and added a configuration that used the sss ID mapping back end to the /etc/samba/smb.conf file to share directories, changes in the ID mapping back end caused errors. Consequently, Samba denied access to files in certain cases, even if the user or group existed and it was known by SSSD. The problem has been fixed. As a result, Samba no longer denies access when using the sss plug-in.

(BZ#1657665)

5.7. COMPILERS AND DEVELOPMENT TOOLS

GCC rebased to version 8.3.1
The GNU Compiler Collection (GCC) has been updated to upstream version 8.3.1. This version brings a large number of miscellaneous bug fixes.

(BZ#1680182)

### 5.8. FILE SYSTEMS AND STORAGE

**FCoE LUNs do not disappear after being created on the bnx2fc cards**

Previously, after creating a FCoE LUN on the bnx2fc cards, the FCoE LUNs were not attached correctly. As a consequence, FCoE LUNs disappeared after being created on the bnx2fc cards on RHEL 8.0. With this update, FCoE LUNs are attached correctly. As a result, it is now possible to discover the FCoE LUNs after they are created on the bnx2fc cards.

(BZ#1685894)

**VDO volumes no longer lose deduplication advice after moving to a different-endian platform**

Previously, the Universal Deduplication Service (UDS) index lost all deduplication advice after moving the VDO volume to a platform that used a different endian. As a consequence, VDO was unable to deduplicate newly written data against the data that was stored before you moved the volume, leading to lower space savings.

With this update, you can now move VDO volumes between platforms that use different endians without losing deduplication advice.

(BZ#1696492)

### 5.9. NETWORKING

**The kernel now supports destination MAC addresses in bitmap:ipmac, hash:ipmac, and hash:mac IP set types**

Previously, the kernel implementation of the bitmap:ipmac, hash:ipmac, and hash:mac IP set types only allowed matching on the source MAC address, while destination MAC addresses could be specified, but were not matched against set entries. As a consequence, administrators could create iptables rules that used a destination MAC address in one of these IP set types, but packets matching the given specification were not actually classified. With this update, the kernel compares the destination MAC address and returns a match if the specified classification corresponds to the destination MAC address of a packet. As a result, rules that match packets against the destination MAC address now work correctly.

(BZ#1649087)

**The TRACE target in the iptables-extensions(8) man page has been updated**

Previously, the description of the TRACE target in the iptables-extensions(8) man page referred only to the compat variant, but Red Hat Enterprise Linux 8.0 uses the nf_tables variant. As a consequence, the man page did not reference the xtables-monitor command-line utility to display TRACE events. The man page has been updated and, as a result, now mentions xtables-monitor.

(BZ#1658734)

The /etc/hosts.allow and /etc/hosts.deny files no longer contain outdated references to removed tcp_wrappers
Previously, the `/etc/hosts.allow` and `/etc/hosts.deny` files contained outdated information about the `tcp_wrappers` package. The files are removed in RHEL 8 as they are no longer needed for `tcp_wrappers` which is removed.

(BZ#1663556)

5.10. SECURITY

Unconfined domains can now use `smc_socket`

Previously, the SELinux policy did not have the allow rules for the `smc_socket` class. Consequently, SELinux blocked an access to `smc_socket` for the unconfined domains. With this update, the allow rules have been added to the SELinux policy. As a result, the unconfined domains can use `smc_socket`.

(BZ#1683642)

`curve25519-sha256` is now supported by default in OpenSSH

Previously, the `curve25519-sha256` SSH key exchange algorithm was missing in the system-wide crypto policies configurations for the OpenSSH client and server even though it was compliant with the default policy level. As a consequence, if a client or a server used `curve25519-sha256` and this algorithm was not supported by the host, the connection might fail. This update of the `crypto-policies` package fixes the bug, and SSH connections no longer fail in the described scenario.

(BZ#1678661)

5.11. VIRTUALIZATION

Hot-plugging PCI devices to a pcie-to-pci bridge controller works correctly

Previously, if a guest virtual machine configuration contained a pcie-to-pci-bridge controller that had no endpoint devices attached to it at the time the guest was started, hot-plugging new devices to that controller was not possible. This update improves how hot-plugging legacy PCI devices on a PCIe system is handled, which prevents the problem from occurring.

(BZ#1619884)

Enabling nested virtualization no longer blocks live migration

Previously, the nested virtualization feature was incompatible with live migration. As a consequence, enabling nested virtualization on a RHEL 8 host prevented migrating any virtual machines (VMs) from the host, as well as saving VM state snapshots to disk. This update fixes the described problem, and the impacted VMs are now possible to migrate.

(BZ#1689216)
CHAPTER 6. TECHNOLOGY PREVIEWS

This part provides a list of all Technology Previews available in Red Hat Enterprise Linux 8.1.

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

6.1. KERNEL

The ibmvnic device driver available as a Technology Preview

With Red Hat Enterprise Linux 8.0, the IBM Virtual Network Interface Controller (vNIC) driver for IBM POWER architectures, ibmvnic, is available as a Technology Preview. vNIC is a PowerVM virtual networking technology that delivers enterprise capabilities and simplifies network management. It is a high-performance, efficient technology that when combined with SR-IOV NIC provides bandwidth control Quality of Service (QoS) capabilities at the virtual NIC level. vNIC significantly reduces virtualization overhead, resulting in lower latencies and fewer server resources, including CPU and memory, required for network virtualization.

(BZ#1524683)

Control Group v2 available as a Technology Preview in RHEL 8

Control Group v2 mechanism is a unified hierarchy control group. Control Group v2 organizes processes hierarchically and distributes system resources along the hierarchy in a controlled and configurable manner.

Unlike the previous version, Control Group v2 has only a single hierarchy. This single hierarchy enables the Linux kernel to:

- Categorize processes based on the role of their owner.
- Eliminate issues with conflicting policies of multiple hierarchies.

Control Group v2 supports numerous controllers:

- CPU controller regulates the distribution of CPU cycles. This controller implements:
  - Weight and absolute bandwidth limit models for normal scheduling policy.
  - Absolute bandwidth allocation model for real time scheduling policy.
- Memory controller regulates the memory distribution. Currently, the following types of memory usages are tracked:
  - Userland memory – page cache and anonymous memory.
  - Kernel data structures such as dentries and inodes.
  - TCP socket buffers.
- I/O controller regulates the distribution of I/O resources.
- Writeback controller interacts with both Memory and I/O controllers and is Control Group v2 specific.
The information above was based on link: https://www.kernel.org/doc/Documentation/cgroup-v2.txt. You can refer to the same link to obtain more information about particular Control Group v2 controllers.

(BZ#1401552)

**bcc-tools is provided as a Technology Preview in RHEL 8**

**BPF Compiler Collection (BCC)** is a userspace tool kit for creating efficient kernel tracing and manipulation programs. **BCC** provides tools for I/O analysis, networking, and monitoring of Linux operating systems using the **extended Berkeley Packet Filtering (eBPF)**.

(BZ#1667043)

**eBPF available as a Technology Preview**

The **extended Berkeley Packet Filtering (eBPF)** feature is available as a Technology Preview for both networking and tracing. eBPF enables the user space to attach custom programs onto a variety of points (sockets, trace points, packet reception) to receive and process data. The feature includes a new system call `bpf()`, which supports creating various types of maps, and also to insert various types of programs into the kernel. Note that the `bpf()` syscall can be successfully used only by a user with the `CAP_SYS_ADMIN` capability, such as a root user. See the `bpf(2)` man page for more information.

(BZ#1559616)

### 6.2. 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)

### 6.3. HARDWARE ENABLEMENT

**The igc driver available as a Technology Preview for RHEL 8**

The **igc** Intel 2.5G Ethernet Linux wired LAN driver is now available on all architectures for RHEL 8 as a Technology Preview. The **ethtool** utility also supports **igc** wired LANs.

(BZ#1495358)

### 6.4. 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 Technology Preview.

In Red Hat Enterprise Linux 7.3, the IdM API was enhanced to enable multiple versions of API commands. Previously, 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 to 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).

(DZ#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:

- Secure Domain Name System (DNS) Deployment Guide: http://dx.doi.org/10.6028/NIST.SP.800-81-2

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)

6.5. FILE SYSTEMS AND STORAGE

NVMe/TCP initiator is available as a Technology Preview

The NVMe over TCP (NVMe/TCP) storage transport is now available as a Technology Preview in initiator mode.

Software target mode is not supported. You can use only a hardware target.

(BZ#1683858)

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

In Red Hat Enterprise Linux 8.0, 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.
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. See the Linux kernel documentation for additional information: https://www.kernel.org/doc/Documentation/filesystems/overlayfs.txt.

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. Only the default container engine configuration can be used; that is, 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 userspace behavior are not considered stable, and might see changes 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.

- Commands used with XFS:
  - XFS file systems must be created with the -n ftype=1 option enabled for use as an overlay.
  - With the rootfs and any file systems created during system installation, set the --mkfsoptions=-n ftype=1 parameters in the Anaconda kickstart.
  - When creating a new file system after the installation, run the # mkfs -t xfs -n ftype=1 /PATH/TO/DEVICE command.
To determine whether an existing file system is eligible for use as an overlay, run the `xfs_info /PATH/TO/DEVICE | grep ftype` command to see if the `ftype=1` option is enabled.

- SELinux security labels are enabled by default in all supported container engines with OverlayFS.
- There are several known issues 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.

(BZ#1690207)

**Stratis is now available**

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.

(JIRA:RHELPLAN-1212)

### 6.6. HIGH AVAILABILITY AND CLUSTERS

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

Pacemaker container bundles now run on the `podman` container platform, 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)

### 6.7. NETWORKING

**TIPC available as a Technology Preview**

The Transparent Inter Process Communication (TIPC) is a protocol specially designed for efficient communication within clusters of loosely paired nodes. It works as a kernel module and provides a `tipc` tool in `iproute2` package to allow designers to create applications that can communicate quickly and reliably with other applications regardless of their location within the cluster. This feature is available as a Technology Preview.

(BZ#1581898)

**eBPF for tc available as a Technology Preview**
As a Technology Preview, the Traffic Control (tc) kernel subsystem and the tc tool can attach extended Berkeley Packet Filtering (eBPF) programs as packet classifiers and actions for both ingress and egress queueing disciplines. This enables programmable packet processing inside the kernel network data path.

(BZ#1699825)

**nmstate available as a Technology Preview**

Nmstate is a network API for hosts. The nmstate packages, available as a Technology Preview, provide a library and the nmstatectl command-line utility to manage host network settings in a declarative manner. The networking state is described by a pre-defined schema. Reporting of the current state and changes to the desired state both conform to the schema.

For further details, see the `/usr/share/doc/nmstate/README.md` file and the examples in the `/usr/share/doc/nmstate/examples` directory.

(BZ#1674456)

**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 available as a Technology Preview**

The eXpress Data Path (XDP) feature, which is available as a Technology Preview, provides a means to attach extended Berkeley Packet Filter (eBPF) programs for high-performance packet processing at an early point in the kernel ingress data path, allowing efficient programmable packet analysis, filtering, and manipulation.

(BZ#1503672)

**KTLS available as a Technology Preview**

In Red Hat Enterprise Linux 8, Kernel Transport Layer Security (KTLS) is provided as a Technology Preview. KTLS handles TLS records using the symmetric encryption or decryption algorithms in the kernel for the AES-GCM cipher. KTLS also provides the interface for offloading TLS record encryption to Network Interface Controllers (NICs) that support this functionality.

(BZ#1570255)

### 6.8. VIRTUALIZATION

**Select Intel network adapters now support SR-IOV in RHEL 7 guest OS on Hyper-V**

As a Technology Preview, Red Hat Enterprise Linux 7 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 i40evf 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)

**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 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 introduces 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 15 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, assigning a physical GPU to VMs makes it impossible for the host to use the GPU, and may prevent graphical display output on the host from working.

(BZ#1528684)

**Nested virtualization now available on IBM POWER 9**
As a Technology Preview, it is now possible to use the nested virtualization features on RHEL 8 host machines running on IBM POWER 9 systems. Nested virtualization enables KVM virtual machines (VMs) to act as hypervisors, which allows for running VMs inside VMs.

Note that nested virtualization also remains a Technology Preview on AMD64 and Intel 64 systems.

Also note that for nested virtualization to work on IBM POWER 9, the host, the guest, and the nested guests currently all need to run one of the following operating systems:

- RHEL 8
- RHEL 7 for POWER 9

(BZ#1505999, BZ#1518937)
CHAPTER 7. DEPRECATED FUNCTIONALITY

This part provides an overview of functionality that has been deprecated in Red Hat Enterprise Linux 8.1.

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)

7.2. SOFTWARE MANAGEMENT

The rpmbuild --sign command has been 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. HARDWARE ENABLEMENT

The qla3xxx driver is deprecated

The qla3xxx driver has been deprecated in RHEL 8. The driver will likely not be supported in future major releases of this product, and thus it is not recommended for new deployments.

(BZ#1658840)

The dl2k, dnet, ethoc, and dlci drivers are deprecated

The dl2k, dnet, ethoc, and dlci drivers have been deprecated in RHEL 8. The drivers will likely not be supported in future major releases of this product, and thus they are not recommended for new deployments.

(BZ#1660627)

7.4. FILE SYSTEMS AND STORAGE

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 the following article: Why does the 'elevator=' parameter no longer work in RHEL8.
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.

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.

7.6. SECURITY

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.

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.
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.

7.7. 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. However, in Red Hat Enterprise Linux 8.0, some features may only be accessible from either virt-manager or the command line.

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.

Note that a new VM snapshot mechanism is under development and will be fully implemented in a future minor release of RHEL 8.

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.

7.8. 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
- authd
- custodia
- hostname
• libidn
• net-tools
• network-scripts
• nss-pam-ldapd
• sendmail
• yp-tools
• ypbIND
• ypserve
CHAPTER 8. KNOWN ISSUES

This part describes known issues in Red Hat Enterprise Linux 8.

8.1. THE WEB CONSOLE

Unprivileged users can access the Subscriptions page

If a non-administrator navigates to the Subscriptions page of the web console, the web console displays a generic error message “Cockpit had an unexpected internal error”.

To work around this problem, sign in to the web console with a privileged user and make sure to check the Reuse my password for privileged tasks checkbox.

(BZ#1674337)

8.2. INSTALLER AND IMAGE CREATION

The auth and authconfig Kickstart commands require the AppStream repository

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

To work around this problem, verify that the BaseOS and AppStream repositories are available to the 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)

Installation fails when using the reboot --kexec command

The RHEL 8 installation fails when using a Kickstart file that contains the reboot --kexec command. To avoid the problem, use the reboot command instead of reboot --kexec in your Kickstart file.

(BZ#1672405)

Copying the content of the Binary DVD.iso file to a partition omits the .treeinfo and .discinfo files

During local installation, while copying the content of the RHEL 8 Binary DVD.iso image file to a partition, the * in the cp <path>/A/* <mounted partition>/dir command fails to copy the .treeinfo and .discinfo files. These files are required for a successful installation. As a result, the BaseOS and AppStream repositories are not loaded, and a debug-related log message in the anaconda.log file is the only record of the problem.

To work around the problem, copy the missing .treeinfo and .discinfo files to the partition.
8.3. KERNEL

The i40iw module does not load automatically on boot

Due to many i40e NICs not supporting iWarp and the i40iw module not fully supporting suspend/resume, this module is not automatically loaded by default to ensure suspend/resume works properly. To work around this problem, manually edit the `/lib/udev/rules.d/90-rdma-hw-modules.rules` file to enable automated load of i40iw.

Also note that if there is another RDMA device installed with a i40e device on the same machine, the non-i40e RDMA device triggers the rdma service, which loads all enabled RDMA stack modules, including the i40iw module.

(BZ#1623712)

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)

KSM sometimes ignores NUMA memory policies

When the kernel shared memory (KSM) feature is enabled with the `merge_across_nodes=1` parameter, KSM ignores memory policies set by the `mbind()` function, and may merge pages from some memory areas to Non-Uniform Memory Access (NUMA) nodes that do not match the policies.

To work around this problem, disable KSM or set the `merge_across_nodes` parameter to 0 if using NUMA memory binding with QEMU. As a result, NUMA memory policies configured for the KVM VM will work as expected.

(BZ#1153521)

Debug kernel fails to boot in crash capture environment in RHEL 8

Due to memory-demanding 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 accordingly. As a result, the debug kernel successfully boots in the crash capture environment.

(BZ#1659609)

8.4. SOFTWARE MANAGEMENT

`yum repolist` ends on first unavailable repository with `skip_if_unavailable=false`

The repository configuration option `skip_if_unavailable` is by default set as follows:

```
skip_if_unavailable=false
```
This setting forces the `yum repolist` command to end on first unavailable repository with an error and exit status 1. Consequently, `yum repolist` does not continue listing available repositories.

Note that it is possible to override this setting in each repository’s `*.repo` file.

However, if you want to keep the default settings, you can work around the problem by using `yum repolist` with the following option:

```
--setopt=*:skip_if_unavailable=True
```

(BZ#1697472)

**YUM v4 requires all packages specified with yum install to be available**

YUM v4 validates all arguments of the `yum install` command. Consequently, if any argument does not match an existing package, YUM v4 exits and does not install packages that match. This behavior differs from YUM v3 on RHEL 7 where the matching packages were installed in such situation. To work around the problem and make the matching packages installed, use the `--skip-broken` argument together with `yum install`.

For more information, see [Why does "yum install <package1> <package2>", where the "<package2>" identifier doesn’t exist, cause the transaction to fail in Red Hat Enterprise Linux 8? Knowledgebase article.](BZ#1717429)

**Programs may fail because RPM Python 3 bindings return header string data as string objects**

RPM Python 3 bindings now return header string values as string objects instead of bytes. Consequently, some programs that adapted to the bytes-behavior may now fail on `TypeError`. Currently, there is no workaround available.

(BZ#1631292)

### 8.5. INFRASTRUCTURE SERVICES

**The tuned-adm utility does not always change CPU governor**

When using the `tuned-adm` utility to change the Tuned profile from `throughput-performance` to balanced, CPU governor is not changed from `performance` to `powersave`. To work around the problem, run the following command after switching the Tuned profile to `balanced`:

```
# cpupower frequency-set -governor powersave
```

(BZ#1679205)

### 8.6. SHELLS AND COMMAND-LINE TOOLS

**snmpd does not start due to missing port specification in trapsink**

The default configuration of the `trapsink` statement does not include port specification. Consequently, the `snmpd` service cannot start. To work around the problem, specify the port after destination address, as in the following example:
Applications using Wayland protocol cannot be forwarded to remote display servers

In Red Hat Enterprise Linux 8.1, most applications use the Wayland protocol by default instead of the X11 protocol. As a consequence, the ssh server cannot forward the applications that use the Wayland protocol but is able to forward the applications that use the X11 protocol to a remote display server.

To work around this problem, set the environment variable `GDK_BACKEND=x11` before starting the applications. As a result, the application can be forwarded to remote display servers.

(systemd-resolved.service fails to start on boot)

The `systemd-resolved` service occasionally fails to start on boot. If this happens, restart the service manually after the boot finishes by using the following command:

```
# systemctl start systemd-resolved
```

However, the failure of `systemd-resolved` on boot does not impact any other services.

(nginx cannot load server certificates from hardware security tokens)

The `nginx` web server supports loading TLS private keys from hardware security tokens directly from PKCS#11 modules. However, it is currently impossible to load server certificates from hardware security tokens through the PKCS#11 URI. To work around this problem, store server certificates on the file system.

(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.

(The console prompt is not displayed when running `systemctl isolate multi-user.target`)

When running the `systemctl isolate multi-user.target` command from GNOME Terminal in a GNOME Desktop session, only a cursor is displayed, and not the console prompt. To work around the problem, press the Ctrl+Alt+F2 keys. As a result, the console prompt appears.

The behavior applies both to GNOME Shell on Wayland and X.Org display server.

8.8. DESKTOP
8.9. HARDWARE ENABLEMENT

The HP NMI watchdog in some cases does not generate a crash dump

The `hpwdt` driver for the HP NMI watchdog is sometimes 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. As a consequence, `hpwdt` in some cases cannot call a panic to generate a crash dump.

(BZ#1602962)

An `openmpi` package cannot be installed due to unresolved dependencies.

An `opensm` rebase changed its soname. As a consequence, any package not rebuilt against the updated `opensm` cannot be installed. To partially mitigate the problem, as there is no workaround available, dependent `openmpi` packages need to be rebuilt against it.

Result: RHEL-8.1 Beta will ship with an openmpi and mpitests-openmpi package that cannot be installed.

(BZ#1717289)

8.10. IDENTITY MANAGEMENT

AD users with expired accounts can be allowed to log in when using GSSAPI authentication

The `accountExpires` attribute that SSSD uses to see whether an account has expired is not replicated to the global catalog by default. As a result, users with expired accounts can log in when using GSSAPI authentication. To work around this problem, the global catalog support can be disabled by specifying `ad_enable_gc=False` in the `sssd.conf` file. With this setting, users with expired accounts will be denied access when using GSSAPI authentication.

Note that SSSD connects to each LDAP server individually in this scenario, which can increase the connection count.

(BZ#1081046)

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)

Changing `/etc/nsswitch.conf` requires a manual system reboot

Any change to the `/etc/nsswitch.conf` file, for example running the `authselect select profile_id` command, requires a system reboot so that all relevant processes use the updated version of the `/etc/nsswitch.conf` file. If a system reboot is not possible, restart the service that joins your system to Active Directory, which is the `System Security Services Daemon` (SSSD) or `winbind`.

(BZ#1657295)

No information about required DNS records displayed when enabling support for AD trust in IdM
When enabling support for Active Directory (AD) trust in Red Hat Enterprise Linux Identity Management (IdM) installation with external DNS management, no information about required DNS records is displayed. Forest trust to AD is not successful until the required DNS records are added. To work around this problem, run the `ipa dns-update-system-records --dry-run` command to obtain a list of all DNS records required by IdM. When external DNS for IdM domain defines the required DNS records, establishing forest trust to AD is possible.

(BZ#1665051)

SSSD returns incorrect LDAP group membership for local users

If the System Security Services Daemon (SSSD) serves users from the local files, the files provider does not include group memberships from other domains. As a consequence, if a local user is a member of an LDAP group, the `id local_user` command does not return the user's LDAP group membership. To work around the problem, either revert the order of the databases where the system is looking up the group membership of users in the `/etc/nsswitch.conf` file, replacing `sss files` with `files sss`, or disable the implicit `files` domain by adding `enable_files_domain=False` to the `[sssd]` section in the `/etc/sssd/sssd.conf` file.

As a result, `id local_user` returns correct LDAP group membership for local users.

(BZ#1652562)

Default PAM settings for systemd-user have changed in RHEL 8 which may influence SSSD behavior

The Pluggable authentication modules (PAM) stack has changed in Red Hat Enterprise Linux 8. For example, the `systemd` user session now starts a PAM conversation using the `systemd-user` PAM service. This service now recursively includes the `system-auth` PAM service, which may include the `pam_sss.so` interface. This means that the SSSD access control is always called.

Be aware of the change when designing access control rules for RHEL 8 systems. For example, you can add the `systemd-user` service to the allowed services list.

Please note that for some access control mechanisms, such as IPA HBAC or AD GPOs, the `systemd-user` service is has been added to the allowed services list by default and you do not need to take any action.

(BZ#1669407)

SSSD does not correctly handle multiple certificate matching rules with the same priority

If a given certificate matches multiple certificate matching rules with the same priority, the System Security Services Daemon (SSSD) uses only one of the rules. As a workaround, use a single certificate matching rule whose LDAP filter consists of the filters of the individual rules concatenated with the `|` (or) operator. For examples of certificate matching rules, see the `sss-certamp(5)` man page.

(BZ#1447945)

8.11. FILE SYSTEMS AND STORAGE

Certain SCSI drivers might sometimes use an excessive amount of memory
Certain SCSI drivers use a larger amount of memory than in RHEL 7. In certain cases, such as vPort creation on a Fibre Channel host bus adapter (HBA), the memory usage might be excessive, depending upon the system configuration.

The increased memory usage is caused by memory preallocation in the block layer. Both the multiqueue block device scheduling (BLK-MQ) and the multiqueue SCSI stack (SCSI-MQ) preallocate memory for each I/O request in RHEL 8, leading to the increased memory usage.

(BZ#1698297)

8.12. NETWORKING

The formatting of the verbose output of `arptables` has changed

Previously on RHEL 7, the verbose output of the `arptables` utility separated counter values with both a space and a comma. In RHEL 8.0, the `iptables-arptables` package provides an `nftables`-based replacement of the `arptables` utility, which separates the described output with only a comma. As a consequence, if you use scripts that parse the output of the `arptables -v -L` command, you might have to adjust the scripts to use the changed output. A later version of RHEL 8 will restore the old format.

(BZ#1676968)

`nftables` does not support multi-dimensional IP set types

The `nftables` packet-filtering framework does not support set types with concatenations and intervals. Consequently, you cannot use multi-dimensional IP set types, such as `hash:net,port`, with `nftables`.

To work around this problem, use the `iptables` framework with the `ipset` tool if you require multi-dimensional IP set types.

(BZ#1593711)

8.13. SECURITY

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)

`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:

```bash
# 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)

**Audit transport=KRB5 does not work**

Audit KRB5 transport mode does not work correctly. Consequently, Audit remote logging using the Kerberos peer authentication does not work.

(BZ#1730382)

**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)

**Parameter not known errors in the rsyslog output with config.enabled**

In the `rsyslog` output, an unexpected bug occurs in configuration processing errors using the `config.enabled` directive. As a consequence, parameter not known errors are displayed while using the `config.enabled` directive except for the `include()` statements.

To work around this problem, set `config.enabled=on` or use `include()` statements.

(BZ#1659383)

**TLS 1.3 does not work in NSS in FIPS mode**

TLS 1.3 is not supported on systems working in FIPS mode. As a result, connections that require TLS 1.3 for interoperability do not function on a system working in FIPS mode.

To enable the connections, disable the system’s FIPS mode or enable support for TLS 1.2 in the peer.

(BZ#1724250)

**A utility for security and compliance scanning of containers is not available**

In Red Hat Enterprise Linux 7, the `oscap-docker` utility can be used for scanning of Docker containers based on Atomic technologies. In Red Hat Enterprise Linux 8, the Docker- and Atomic-related OpenSCAP commands are not available. As a result, `oscap-docker` or an equivalent utility for security and compliance scanning of containers is not available in RHEL 8 at the moment.

(BZ#1642373)

**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`:

To work around this problem, use only correctly working priority strings:


As a result, current configurations must be limited to the strings that work correctly.

(BZ#1679512)

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

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

To work around the problem, add the following lines after the .include line at the end of the crypto_policy section in the /etc/pki/tls/openssl.cnf file:

```
MaxProtocol = TLSv1.2
```

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

(BZ#1685470)

OpenSCAP does not provide offline scanning of virtual machines and containers

Refactoring of OpenSCAP codebase caused certain RPM probes to fail to scan VM and containers file systems in offline mode. For that reason, the following tools were removed from the openscap-utils package: oscap-vm and oscap-chroot. Also, the openscap-containers package was completely removed.

(BZ#1618489)

OpenSCAP rpmverifypackage does not work correctly

The chdir and chroot system calls are called twice by the rpmverifypackage probe. Consequently, an error occurs when the probe is utilized during an OpenSCAP scan with custom Open Vulnerability and Assessment Language (OVAL) content.

To work around this problem, do not use the rpmverifypackage_test OVAL test in your content or use only the content from the scap-security-guide package where rpmverifypackage_test is not used.

(BZ#1646197)

SCAP Workbench fails to generate results-based remediations from tailored profiles

The following error occurs when trying to generate results-based remediation roles from a customized profile using the SCAP Workbench tool:

```
Error generating remediation role .../remediation.sh: Exit code of oscap was 1: [output truncated]
```
To work around this problem, use the `oscap` command with the `--tailoring-file` option.

(BZ#1640715)

### 8.14. 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)

### 8.15. VIRTUALIZATION

**Using `cloud-init` to provision virtual machines on Microsoft Azure fails**

Currently, it is not possible to use the `cloud-init` utility to provision a RHEL 8 virtual machine (VM) on the Microsoft Azure platform. To work around this problem, use one of the following methods:

- Use the `WALinuxAgent` package instead of `cloud-init` to provision VMs on Microsoft Azure.
- Add the following setting to the `[main]` section in the `/etc/NetworkManager/NetworkManager.conf` file:
  ```
  [main]
dhcp=dhclient
  ```

(BZ#1641190)

**Low GUI display performance in RHEL 8 virtual machines on a Windows Server 2019 host**

When using RHEL 8 as a guest operating system in graphical mode on a Windows Server 2019 host, the GUI display performance is low, and connecting to a console output of the guest currently takes significantly longer than expected.

This is a known issue on Windows 2019 hosts and is pending a fix by Microsoft. To work around this problem, connect to the guest using SSH or use Windows Server 2016 as the host.

(BZ#1706541)

**Installing RHEL virtual machines sometimes fails**

Under certain circumstances, RHEL 7 and RHEL 8 virtual machines created using the `virt-install` utility fail to boot if the `--location` option is used.

To work around this problem, use the `--extra-args` option instead and specify an installation tree reachable by the network, for example:

```
--extra-args="inst.repo=https://some/url/tree/path"
```

This ensures that the RHEL installer finds the installation files correctly.
Displaying multiple monitors of virtual machines that use Wayland is not possible with QXL

Using the `remote-viewer` utility to display more than one monitor of a virtual machine (VM) that is using the Wayland display server causes the VM to become unresponsive and the *Waiting for display* status message to be displayed indefinitely.

To work around this problem, use `virtio-gpu` instead of `qxl` as the GPU device for VMs that use Wayland.

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.

RHEL 8 virtual machines sometimes cannot boot on Witherspoon hosts

RHEL 8 virtual machines (VMs) that use the *pseries-rhel7.6.0-sxxm* machine type in some cases fail to boot on *Power9 S922LC for HPC* hosts, also known as Witherspoon.

Attempting to boot such a VM instead generates the following error message:

```
qemu-kvm: Requested safe indirect branch capability level not supported by kvm, try cap-ibs=fixed-ibs
```

To work around this problem, add one of the following strings to the kernel command line of the VM:

- `pseries-rhel7.6.0-sxxm,cap-ibs=fixed-ibs`
- `pseries-rhel7.6.0-sxxm,cap-ibs=broken`

IBM POWER virtual machines do not work correctly with zero memory NUMA nodes

Currently, when an IBM POWER virtual machine (VM) running on a RHEL 8 host is configured with a NUMA node that uses zero memory (`memory='0'`), the VM does not work correctly. As a consequence, Red Hat strongly recommends not using IBM POWER VMs with zero-memory NUMA nodes on RHEL 8.
CHAPTER 9. NOTABLE CHANGES TO CONTAINERS

A set of container images is available for Red Hat Enterprise Linux (RHEL) 8.1 Beta. Notable changes include:

- Rootless containers are available as a Technology Preview in RHEL 8.1 Beta. Rootless containers are containers that are created and managed by regular system users without administrative permissions. This allows users to maintain their identity, including such things as credentials to container registries.

You can try rootless containers using the podman and buildah commands. For further information:

  - for rootless containers, see How does rootless Podman work.
  - for buildah, see Building container images with Buildah.
  - for podman, see Building, running, and managing containers.

- As of RHEL 8.1 Beta, you can add the toolbox RPM package your RHEL system. The toolbox command is a utility often used with container-oriented operating systems, such as Red Hat CoreOS. With toolbox, you can troubleshoot and debug host operating systems by launching a container that includes a large set of troubleshooting tools for you to use, without having to install those tools on the host system.

  Running the toolbox command starts a rhel-tools container that provides root access to the host, for fixing or otherwise working with that host.

- The podman package has been upgraded to upstream version 1.4.2. For information on features added to podman since version 1.0.0, which was used in RHEL 8.0, refer to descriptions of the latest podman releases on Github.
CHAPTER 10. INTERNATIONALIZATION

10.1. 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.

- European Languages - English, German, Spanish, French, Italian, Portuguese, and Russian.

The following table lists the fonts and input methods provided for various major languages.

<table>
<thead>
<tr>
<th>Language</th>
<th>Default Font (Font Package)</th>
<th>Input Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>dejavu-sans-fonts</td>
<td></td>
</tr>
<tr>
<td>French</td>
<td>dejavu-sans-fonts</td>
<td></td>
</tr>
<tr>
<td>German</td>
<td>dejavu-sans-fonts</td>
<td></td>
</tr>
<tr>
<td>Italian</td>
<td>dejavu-sans-fonts</td>
<td></td>
</tr>
<tr>
<td>Russian</td>
<td>dejavu-sans-fonts</td>
<td></td>
</tr>
<tr>
<td>Spanish</td>
<td>dejavu-sans-fonts</td>
<td></td>
</tr>
<tr>
<td>Portuguese</td>
<td>dejavu-sans-fonts</td>
<td></td>
</tr>
<tr>
<td>Simplified Chinese</td>
<td>google-noto-sans-cjk-ttc-fonts,</td>
<td>ibus-libpinyin, libpinyin</td>
</tr>
<tr>
<td></td>
<td>google-noto-serif-cjk-ttc-fonts</td>
<td></td>
</tr>
<tr>
<td>Traditional Chinese</td>
<td>google-noto-sans-cjk-ttc-fonts,</td>
<td>ibus-libzhuyin, libzhuyin</td>
</tr>
<tr>
<td></td>
<td>google-noto-serif-cjk-ttc-fonts</td>
<td></td>
</tr>
<tr>
<td>Japanese</td>
<td>google-noto-sans-cjk-ttc-fonts,</td>
<td>ibus-kkc, libkkc</td>
</tr>
<tr>
<td></td>
<td>google-noto-serif-cjk-ttc-fonts</td>
<td></td>
</tr>
<tr>
<td>Korean</td>
<td>google-noto-sans-cjk-ttc-fonts,</td>
<td>ibus-hangul, libhangu</td>
</tr>
<tr>
<td></td>
<td>google-noto-serif-cjk-ttc-fonts</td>
<td></td>
</tr>
</tbody>
</table>

10.2. 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.
- The **glibc** package updates for multiple locales are now synchronized with the Common Locale Data Repository (CLDR).
### APPENDIX A. LIST OF TICKETS BY COMPONENT

<table>
<thead>
<tr>
<th>Component</th>
<th>Tickets</th>
</tr>
</thead>
<tbody>
<tr>
<td>anaconda</td>
<td>BZ#1628653, BZ#1673901, BZ#1671047, BZ#1689909, BZ#1689194, BZ#1584145, BZ#1672405, BZ#1687747, BZ#1655523</td>
</tr>
<tr>
<td>audit</td>
<td>BZ#1730382</td>
</tr>
<tr>
<td>authselect</td>
<td>BZ#1657295</td>
</tr>
<tr>
<td>bcc</td>
<td>BZ#1667043</td>
</tr>
<tr>
<td>bpftrace</td>
<td>BZ#1687802</td>
</tr>
<tr>
<td>chrony</td>
<td>BZ#1685469</td>
</tr>
<tr>
<td>cloud-init</td>
<td>BZ#1641190</td>
</tr>
<tr>
<td>cockpit-appstream</td>
<td>BZ#1658847</td>
</tr>
<tr>
<td>cockpit</td>
<td>BZ#1678956, BZ#1657752, BZ#1678473</td>
</tr>
<tr>
<td>corosync</td>
<td>BZ#1693491</td>
</tr>
<tr>
<td>criu</td>
<td>BZ#1689746</td>
</tr>
<tr>
<td>crypto-policies</td>
<td>BZ#1678661, BZ#1660839</td>
</tr>
<tr>
<td>distribution</td>
<td>BZ#1685191</td>
</tr>
<tr>
<td>dnf</td>
<td>BZ#1717429</td>
</tr>
<tr>
<td>elfutils</td>
<td>BZ#1683705</td>
</tr>
<tr>
<td>enscript</td>
<td>BZ#1664366</td>
</tr>
<tr>
<td>freeradius</td>
<td>BZ#1685546</td>
</tr>
<tr>
<td>frr</td>
<td>BZ#1657029</td>
</tr>
<tr>
<td>gcc-toolset-9</td>
<td>BZ#1685482</td>
</tr>
<tr>
<td>gcc</td>
<td>BZ#1680182</td>
</tr>
<tr>
<td>gdm</td>
<td>BZ#1678627</td>
</tr>
</tbody>
</table>
### APPENDIX A. LIST OF TICKETS BY COMPONENT

<table>
<thead>
<tr>
<th>Component</th>
<th>Tickets</th>
</tr>
</thead>
<tbody>
<tr>
<td>glibc</td>
<td>BZ#1577438</td>
</tr>
<tr>
<td>gnome-shell-extensions</td>
<td>BZ#1717947</td>
</tr>
<tr>
<td>gnome-shell</td>
<td>BZ#1704360</td>
</tr>
<tr>
<td>gnutls</td>
<td>BZ#1628553</td>
</tr>
<tr>
<td>ipa</td>
<td>BZ#1665051, BZ#1719767, JIRA:RHELPLAN-15036, BZ#1664719, BZ#1664718</td>
</tr>
<tr>
<td>iptables</td>
<td>BZ#1658734, BZ#1676968</td>
</tr>
<tr>
<td>kernel-rt</td>
<td>BZ#1678887</td>
</tr>
<tr>
<td>kernel</td>
<td>BZ#1649087, BZ#1564427, BZ#1686755, BZ#1706541, BZ#1666538, BZ#16685894, BZ#1643980, BZ#1602962, BZ#1153521, BZ#1698297, BZ#1348508, BZ#1651474, BZ#170480, BZ#1634343, BZ#1652222, BZ#1687459, BZ#1571628, BZ#1571534, BZ#1685552, BZ#1663281, BZ#1524683, BZ#1519039, BZ#1581898, BZ#1627455, BZ#1501618, BZ#1401552, BZ#1683858, BZ#1495358, BZ#1633143, BZ#1503672, BZ#1505999, BZ#150255, BZ#1665295, BZ#1658840, BZ#1660627</td>
</tr>
<tr>
<td>kexec-tools</td>
<td>BZ#1662911, BZ#1520209, BZ#1710288</td>
</tr>
<tr>
<td>keycloak-httpd-client-install</td>
<td>BZ#1553890</td>
</tr>
<tr>
<td>kmod-kvdo</td>
<td>BZ#1696492</td>
</tr>
<tr>
<td>libdnf</td>
<td>BZ#1697472</td>
</tr>
<tr>
<td>libsemanage</td>
<td>BZ#1666328</td>
</tr>
<tr>
<td>libssh</td>
<td>BZ#1610883</td>
</tr>
<tr>
<td>libstoragemgmt</td>
<td>BZ#1626415</td>
</tr>
<tr>
<td>libvirt</td>
<td>BZ#1528684</td>
</tr>
<tr>
<td>linuxptp</td>
<td>BZ#1677217, BZ#1685467</td>
</tr>
<tr>
<td>lorax</td>
<td>BZ#1663950, BZ#1709594, BZ#1689140</td>
</tr>
<tr>
<td>Component</td>
<td>Tickets</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>lvm2</td>
<td>BZ#1649086</td>
</tr>
<tr>
<td>net-snmp</td>
<td>BZ#1677192</td>
</tr>
<tr>
<td>nfs-utils</td>
<td>BZ#1592011</td>
</tr>
<tr>
<td>nftables</td>
<td>BZ#1593711</td>
</tr>
<tr>
<td>nginx</td>
<td>BZ#1668717, BZ#1690292</td>
</tr>
<tr>
<td>nmstate</td>
<td>BZ#1674456</td>
</tr>
<tr>
<td>nss</td>
<td>BZ#1724250, BZ#1645153</td>
</tr>
<tr>
<td>openmpi</td>
<td>BZ#1717289</td>
</tr>
<tr>
<td>openscap</td>
<td>BZ#1642373, BZ#1618489, BZ#1646197, BZ#1718826, BZ#1709429</td>
</tr>
<tr>
<td>openssh</td>
<td>BZ#1691045</td>
</tr>
<tr>
<td>openssl</td>
<td>BZ#1685470</td>
</tr>
<tr>
<td>pcs</td>
<td>BZ#1619620</td>
</tr>
<tr>
<td>perl-IO-Socket-SSL</td>
<td>BZ#1632600</td>
</tr>
<tr>
<td>perl-Net-SSLeay</td>
<td>BZ#1632597</td>
</tr>
<tr>
<td>perl-Socket</td>
<td>BZ#1699793</td>
</tr>
<tr>
<td>php</td>
<td>BZ#1653109</td>
</tr>
<tr>
<td>pki-core</td>
<td>BZ#1695302, BZ#1729215</td>
</tr>
<tr>
<td>pykickstart</td>
<td>BZ#1637872</td>
</tr>
<tr>
<td>qemu-kvm</td>
<td>BZ#1619884, BZ#1689216, BZ#1651994</td>
</tr>
<tr>
<td>rng-tools</td>
<td>BZ#1692435</td>
</tr>
<tr>
<td>rpm</td>
<td>BZ#1631292, BZ#1688849</td>
</tr>
<tr>
<td>rsyslog</td>
<td>JIRA:RHELPLAN-10431, BZ#1659383, BZ#1679512</td>
</tr>
<tr>
<td>rt-tests</td>
<td>BZ#1686494, BZ#1707505, BZ#1666351</td>
</tr>
</tbody>
</table>
## Component

<table>
<thead>
<tr>
<th>Component</th>
<th>Tickets</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruby-2.6-module</td>
<td>BZ#1672575</td>
</tr>
<tr>
<td>scap-security-guide</td>
<td>BZ#1718839</td>
</tr>
<tr>
<td>scap-workbench</td>
<td>BZ#1640715</td>
</tr>
<tr>
<td>selinux-policy</td>
<td>BZ#1683642, BZ#1673056, BZ#1684103, BZ#1673107</td>
</tr>
<tr>
<td>setools</td>
<td>BZ#1672631</td>
</tr>
<tr>
<td>setup</td>
<td>BZ#1663556</td>
</tr>
<tr>
<td>sssd</td>
<td>BZ#1081046, BZ#1657665, BZ#1652562, BZ#1669407, BZ#1447945</td>
</tr>
<tr>
<td>subscription-manager</td>
<td>BZ#1674337</td>
</tr>
<tr>
<td>systemd</td>
<td>BZ#1658691, BZ#1686892, BZ#1640802</td>
</tr>
<tr>
<td>systemtap</td>
<td>BZ#1675740</td>
</tr>
<tr>
<td>tpm2-abrm-selinux</td>
<td>BZ#1642000</td>
</tr>
<tr>
<td>tpm2-tools</td>
<td>BZ#1664498</td>
</tr>
<tr>
<td>tuned</td>
<td>BZ#1679205, BZ#1685585</td>
</tr>
<tr>
<td>udica</td>
<td>BZ#1673643</td>
</tr>
<tr>
<td>vdo</td>
<td>BZ#1669534</td>
</tr>
<tr>
<td>virt-manager</td>
<td>BZ#1677019</td>
</tr>
<tr>
<td>virtio-win</td>
<td>BZ#1223668</td>
</tr>
<tr>
<td>xorg-x11-drq-qxl</td>
<td>BZ#1642887</td>
</tr>
<tr>
<td>xorg-x11-server</td>
<td>BZ#1687489, BZ#1698565</td>
</tr>
<tr>
<td>other</td>
<td>BZ#1640697, BZ#1623712, BZ#1659609, BZ#1687900, BZ#1697896, BZ#1664592, BZ#1732726, BZ#1731502, BZ#1649493, BZ#1718422, BZ#1690207, JIRA:RHELPLAN-1212, BZ#1559616, BZ#1699825, BZ#1642765, JIRA:RHELPLAN-10304, BZ#1646541, BZ#1647725, BZ#1686057, JIRA:RHELPLAN-13074, JIRA:RHELPLAN-13068, JIRA:RHELPLAN-13066, JIRA:RHELPLAN-2542</td>
</tr>
</tbody>
</table>