



# Red Hat Enterprise Linux 8

## 8.3 发行注记

Red Hat Enterprise Linux 8.3 发行注记



# Red Hat Enterprise Linux 8 8.3 发行注记

---

Red Hat Enterprise Linux 8.3 发行注记

## 法律通告

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

XFS<sup>®</sup> is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack<sup>®</sup> Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

## 摘要

本发行注记提供了在 Red Hat Enterprise Linux 8.3 和文档中已知问题改进和附加组件的高级信息,以及重要的程序错误修复、技术预览、已弃用的功能和其他详情。

# 目录

对红帽文档提供反馈 .....	3
<b>第 1 章 概述</b> .....	<b>4</b>
安装程序和镜像创建	4
RHEL for Edge	4
基础架构服务	4
安全性	4
动态编程语言、网页和数据库服务器	4
编译器工具集	5
Identity Management	5
Web 控制台	5
虚拟化	5
桌面和图形	5
原位升级和操作系统转换	5
OpenJDK 11 现已正式发布	6
其它资源	6
红帽客户门户网站 Labs	6
<b>第 2 章 构架</b> .....	<b>8</b>
<b>第 3 章 RHEL 8 中的内容发布</b> .....	<b>9</b>
3.1. 安装	9
3.2. 软件仓库	9
3.3. 应用程序流	9
3.4. 使用 YUM/DNF 的软件包管理	10
<b>第 4 章 RHEL 8.3.1 发行版本</b> .....	<b>11</b>
4.1. 新特性	11
<b>第 5 章 RHEL 8.3.0 发行版本</b> .....	<b>15</b>
5.1. 新特性	15
5.2. 对外部内核参数的重要更改	63
5.3. 设备驱动程序	67
5.4. 程序错误修复	69
5.5. 技术预览	81
5.6. 过时的功能	90
5.7. 已知问题	98
<b>第 6 章 国际化</b> .....	<b>121</b>
6.1. RED HAT ENTERPRISE LINUX 8 国际语言	121
6.2. RHEL 8 中国际化的显著变化	121
<b>附录 A. 按组件划分的问题单列表</b> .....	<b>122</b>
<b>附录 B. 修订历史</b> .....	<b>130</b>



---

## 对红帽文档提供反馈

我们感谢您对文档提供反馈信息。请让我们了解如何改进文档。要做到这一点：

### 通过 Jira 提交反馈（需要帐户）

1. 登录到 [Jira](#) 网站。
2. 单击顶部导航栏中的 **Create**。
3. 在 **Summary** 字段中输入描述性标题。
4. 在 **Description** 字段中输入您对改进的建议。包括到文档相关部分的链接。
5. 点对话框底部的 **Create**。

# 第 1 章 概述

## 安装程序和镜像创建

在 RHEL 8.3 中，您可以在安装开始前配置 root 密码并创建用户帐户。之前，您需要在安装过程开始后配置一个 root 密码并创建用户帐户。您还可以基于更可靠的后端创建自定义镜像，并通过 RHEL web 控制台将镜像推送到云中。

## RHEL for Edge

RHEL 8.3 引进了在 **Edge** 服务器中远程安装 RHEL 的 RHEL for Edge。RHEL for Edge 是一个 rpm-ostree 镜像，您可以使用 Image Builder 进行编写。您可以首先使用 Kickstart 文件安装镜像，然后可以管理镜像以包含镜像更新，并可以将镜像回滚到之前的功能状态。

以下是 RHEL for Edge 的关键亮点：

- 原子升级，每个更新的状态都是已知的，在重新引导该设备前不会看到任何变化。
- 自定义健康检查和智能回滚以确保弹性。
- 以容器为主的工作流，可将核心操作系统更新与应用程序更新分开，并测试和部署不同的应用程序版本。
- 为低带宽环境优化 OTA 有效负载。

如需更多信息，请参阅 [第 5.1.2 节 “RHEL for Edge”](#)。

## 基础架构服务

Tuned 系统调优工具已更新至版本 2.13，它增加了对架构独立调整和多个包含指令的支持。

## 安全性

RHEL 8.3 使用 **Clevis** 和 **Tang** 为基于策略的解密(PBD)解决方案的自动部署提供了 Ansible 角色，此版本的 **rhel-system-roles** 软件包还包含通过 **Rsyslog** 进行 RHEL 日志记录的 Ansible 角色。

**scap-security-guide** 软件包已被 rebase 到版本 0.150，**OpenSCAP** 被 rebase 到版本 1.3.3。这些更新提供了大量改进，包括与 CIS RHEL 7 Benchmark v2.2.0 相符的配置集，以及符合北美健保机构所要求的 Health Insurance Portability and Accountability Act (HIPAA) 的配置集。

在这个版本中，您可以使用 **SCAP Workbench** 工具从定制的配置集生成基于结果的补救角色。

**USBGuard** 框架现在提供自己的 SELinux 策略，它使用 GUI 通知桌面用户，版本 0.7.8 还包括很多其他改进和程序错误修复。

## 动态编程语言、网页和数据库服务器

以下组件的更新版本现在作为新的模块流提供：

- nginx 1.18
- Node.js 14
- Perl 5.30
- PHP 7.4
- Ruby 2.7

RHEL 8.3 中更新了以下组件：



- **Git** 升级到 2.27
- **Squid** 升级到 4.11 版本

如需更多信息，请参阅 [第 5.1.11 节“动态编程语言、网页和数据库服务器”](#)。

## 编译器工具集

RHEL 8.3 中更新了以下编译器工具集：

- **GCC Toolset 10**
- **LLVM Toolset 10.0.1**
- **Rust Toolset 1.45.2**
- **Go Toolset 1.14.7**

如需更多信息，请参阅 [第 5.1.12 节“编译器和开发工具”](#)。

## Identity Management

RHEL 8 中弃用了 Rivest Cipher 4 (RC4) 加密套件，用户的默认加密类型、服务以及 AD 林中的 Active Directory (AD) 域之间的信任。出于兼容性的原因，这个更新引进了一个新的加密子策略 **AD-SUPPORT**，来启用对已弃用的 RC4 加密类型的支持。新的子策略允许您将 RC4 与 RHEL 身份管理 (IdM) 和 SSSD 活动目录集成解决方案一起使用。

如需更多信息，请参阅 [第 5.1.13 节“身份管理”](#)。

## Web 控制台

Web 控制台提供了一个选项，可以在管理访问和用户会话内的有限访问之间进行切换。

## 虚拟化

IBM Z 硬件上托管的虚拟机 (VM) 现在可以使用 IBM Secure Execution 功能。这样，当主机的安全被破坏时，可以防止虚拟机被攻击，并防止不信任的主机从虚拟机获取信息。另外，DASD 设备现在可以分配给 IBM Z 上的虚拟机。

## 桌面和图形

您现在可以在 IBM Z 系统中使用 GNOME 桌面。

**Direct Rendering Manager (DRM)** 内核图形子系统已被 rebase 到上游 Linux kernel 版本 5.6。与之前的版本相比，这个版本提供了很多改进，包括对新 GPU 和 APU 以及各种驱动程序更新的支持。

详情请查看 [第 5.1.14 节“Desktop”](#) 和 [第 5.1.15 节“图形基础结构”](#)。

## 原位升级和操作系统转换

### RHEL 7 原位升级到 RHEL 8

目前支持的原位升级路径包括：

- 64 位 Intel、IBM POWER 8 (little endian) 和 IBM Z 架构上，从 RHEL 7.8 升级到 RHEL 8.2
- 在需要内核版本 4.14 的架构上，从 RHEL 7.6 到 RHEL 8.2：IBM POWER 9 (little endian) 和 IBM Z (Structure A)
- 在使用 SAP HANA 的系统上，从 RHEL 7.7 升级到 RHEL 8.2。

要确保您的系统在升级到 RHEL 8.2 后仍然被支持，您可以升级到最新的 RHEL 8.3 版本，或启用 RHEL 8.2 延长更新支持(EUS)存储库。在带有 SAP HANA 的系统上，启用 SAP Solutions(E4S)存储库的 RHEL 8.2 更新服务。

如需更多信息，请参阅[支持的 Red Hat Enterprise Linux 原位升级路径](#)。有关执行原位升级的步骤，请参阅[从 RHEL 7 升级到 RHEL 8](#)。

主要改进包括：

- **Leapp** 现在通过生成 true/false 问题来确定如何进行升级来支持用户输入。
- 现在，您可以使用 Satellite Web UI 同时升级多个主机。
- 现在，使用 Red Hat Update Infrastructure (RHUI)，AWS 和 Microsoft Azure 上的 on-demand 实例支持原位升级。
- 发布 [RHBA-2021:0569](#) 公告后，您可以为 **Leapp** 预升级报告创建自定义脚本。详情请参阅 [自动化您的 Red Hat Enterprise Linux 预升级报告 workflow](#)。

## 从 RHEL 6 原位升级到 RHEL 8

要从 RHEL 6.10 升级到 RHEL 8.2，请参阅 [从 RHEL 6 升级到 RHEL 8 部分](#)。

## 从不同的 Linux 发行版转换到 RHEL

如果您使用 CentOS Linux 8 或 Oracle Linux 8，您可以使用红帽支持的 **Convert2RHEL** 工具将您的操作系统转换为 RHEL 8。如需更多信息，请参阅[从基于 RPM 的 Linux 发行版转换到 RHEL](#)。

如果您使用早期版本的 CentOS Linux 或 Oracle Linux（称为版本 6 或 7），可以将操作系统转换为 RHEL，然后执行 RHEL 8 的原位升级。请注意，CentOS Linux 6 和 Oracle Linux 6 的转换使用不被支持的 **Convert2RHEL** 工具。如需有关不支持转换的更多信息，请参阅[如何从 CentOS Linux 6 或 Oracle Linux 6 转换到 RHEL 6](#)。

有关红帽如何支持从其他 Linux 发行本转换到 RHEL 的详情，请参考 [Convert2RHEL 支持政策文档](#)。

## OpenJDK 11 现已正式发布

现在提供了 Open Java Development Kit (OpenJDK) 的新版本。有关本发行版本中引入的功能以及现有功能中变化的更多信息，请参阅 [OpenJDK 11 文档](#)。

## 其它资源

- [Red Hat Enterprise Linux technology capabilities and limits](#) 包括了与其他版本系统相比的 Red Hat Enterprise Linux 8 的能力和限制。
- 有关 Red Hat Enterprise Linux **生命周期** 的详情请查看 [Red Hat Enterprise Linux 生命周期文档](#)。
- [软件包清单文档](#) 为 RHEL 8 提供软件包列表。
- RHEL 7 和 RHEL 8 的主要区别包括在使用 [RHEL 8 时的注意事项](#)。
- [从 RHEL 7 升级到 RHEL 8](#) 文档提供了有关如何执行 [从 RHEL 7 原位升级到 RHEL 8](#) 的说明。
- **Red Hat Insights** 服务可让您主动发现、检查并解决已知的技术问题，所有 RHEL 订阅都可以使用它。有关如何安装 Red Hat Insights 客户端并将您的系统注册到该服务的说明，请查看 [Red Hat Insights 入门页面](#)。

## 红帽客户门户网站 Labs

---

红帽客户门户网站 Labs 是客户门户网站的一个部分中的一组工具，地址为 <https://access.redhat.com/labs/>。红帽客户门户网站 Labs 中的应用程序可帮助您提高性能、快速解决问题、发现安全问题以及快速部署和配置复杂应用程序。一些最常用的应用程序有：

- [Registration Assistant](#)
- [Product Life Cycle Checker](#)
- [Kickstart Generator](#)
- [Kickstart Converter](#)
- [Red Hat Enterprise Linux Upgrade Helper](#)
- [Red Hat Satellite Upgrade Helper](#)
- [Red Hat Code Browser](#)
- [JVM Options Configuration Tool](#)
- [Red Hat CVE Checker](#)
- [Red Hat Product Certificates](#)
- [Load Balancer Configuration Tool](#)
- [Yum Repository Configuration Helper](#)

## 第 2 章 构架

Red Hat Enterprise Linux 8.3 与内核版本 4.18.0-240 一同发布，它支持以下构架：

- AMD 和 Intel 64 位构架
- 64 位 ARM 架构
- IBM Power Systems, Little Endian
- 64-bit IBM Z

请确定为每个构架购买正确的订阅。如需更多信息,请参阅 [Red Hat Enterprise Linux 入门 - 附加构架](#)。有关可用订阅列表, 请查看客户门户网站中的 [订阅使用](#)。

## 第 3 章 RHEL 8 中的内容发布

### 3.1. 安装

Red Hat Enterprise Linux 8 使用 ISO 镜像安装。AMD64、Intel 64 位、64 位 ARM、IBM Power Systems 和 IBM Z 架构有两种类型的 ISO 镜像：

- 二进制 DVD ISO：包含 BaseOS 和 AppStream 软件仓库的完整安装镜像,并允许您在没有附加软件仓库的情况下完成安装。



#### 注意

二进制 DVD ISO 镜像大于 4.7 GB，因此它可能不适用于单层 DVD。当使用二进制 DVD ISO 镜像创建可引导安装介质时，建议使用双层 DVD 或者 USB 设备。您还可以使用 Image Builder 工具创建自定义的 RHEL 镜像。有关镜像构建器的更多信息，请参阅 [编写自定义的 RHEL 系统镜像](#) 文档。

- 引导 ISO：用来引导到安装程序的最小引导 ISO 镜像。这个选项需要访问 BaseOS 和 AppStream 软件仓库来安装软件包。软件仓库是二进制 DVD ISO 镜像的一部分。

有关下载 ISO 镜像、创建安装介质和完成 RHEL 安装的说明，请参阅 [执行标准的 RHEL 8 安装](#) 文档。有关自动 Kickstart 安装和其他高级主题，请参阅 [执行高级的 RHEL 8 安装](#) 文档。

### 3.2. 软件仓库

Red Hat Enterprise Linux 8 由两个主要软件仓库发布：

- BaseOS
- AppStream

两个软件仓库都需要一个基本的 RHEL 安装，所有 RHEL 订阅都包括它们。

BaseOS 仓库的内容旨在提供底层操作系统功能的核心组件，为所有安装提供基础操作系统的基础。这部分内容采用 RPM 格式，它的支持条款与之前的 RHEL 版本相似。有关通过 BaseOS 分发的软件包列表，请查看 [软件包清单](#)。

Application Stream 仓库的内容包括额外的用户空间应用程序、运行时语言和数据库来支持各种工作负载和使用案例。应用程序流以熟悉的 RPM 格式，作为 RPM 格式的扩展提供，称为 *模块*，或作为软件集合。有关 AppStream 中提供的软件包的列表，请查看 [软件包清单](#)。

另外，所有 RHEL 订阅都可以使用 CodeReady Linux Builder 软件仓库。它为开发人员提供了额外的软件包。不支持包括在 CodeReady Linux Builder 存储库中的软件包。

有关 RHEL 8 软件仓库的详情，请查看 [软件包清单](#)。

### 3.3. 应用程序流

Red Hat Enterprise Linux 8 引进了应用程序流（Application Streams）的概念。和操作系统软件包相比，现在为用户空间组件提供了多个版本且会更频繁地进行更新。这为自定义 Red Hat Enterprise Linux 提供了更大的灵活性，不会影响平台或特定部署的基本稳定性。

作为 Application Streams 提供的组件可打包为模块 (module) 或 RPM 软件包，并通过 RHEL 8 中的 AppStream 软件仓库提供。每个 Application Stream 组件都有其特定的生命周期，可能和 RHEL 8 的生命周期相同或更短。详情请查看 [Red Hat Enterprise Linux 生命周期](#)。

模块是代表逻辑单元的软件包集合：应用程序、语言堆栈、数据库或一组工具。这些软件包被一同构建、测试并发布。

模块流代表 Application Stream 组件的版本。例如，PostgreSQL 数据库服务器的几个流 (版本) 在带有默认的 `postgresql:10` 流的 `postgresql` 模块中提供。在系统中只能安装一个模块流。不同的容器可以使用不同的版本。

详细的模块命令，请参考 [安装、管理和删除用户空间组件](#) 文档。有关 AppStream 中提供的模块的列表，请查看 [软件包清单](#)。

### 3.4. 使用 YUM/DNF 的软件包管理

在 Red Hat Enterprise Linux 8 上，安装软件是由 YUM 工具来保证的，该工具基于 DNF 技术。我们有意坚持使用 `yum` 术语，以便与以前的 RHEL 主版本保持一致。但是，如果您输入 `dnf` 而不是 `yum`，则命令可以按预期工作，因为 `yum` 是 `dnf` 的别名，以便兼容。

如需了解更多详细信息，请参阅以下文档：

- [安装、管理和删除用户空间组件](#)
- [使用 RHEL 8 时的注意事项](#)

## 第 4 章 RHEL 8.3.1 发行版本

红帽在次发行版本（8.Y）之间会每季度提供一次 Red Hat Enterprise Linux 8 的内容。每季度发布的版本使用第三个数字(8.Y.1)进行编号。RHEL 8.3.1 版本中的新功能如下所述。

### 4.1. 新特性

#### 用于多个桌面应用程序的 flatpak 软件包

flatpak 是一个系统，用于将图形应用程序作为容器运行。使用 Flatpak，您可以独立于主机操作系统安装和更新应用。

这个更新在 Red Hat Container Catalog 中提供了以下应用程序的 Flatpak 容器镜像：

应用程序名称	Flatpak 容器 ID
Firefox	org.mozilla.firefox
GIMP	org.gimp.GIMP
Inkscape	org.inkscape.Inkscape
Thunderbird	org.mozilla.Thunderbird

要在 Red Hat Container Catalog 中安装 Flatpak 容器，请使用以下步骤：

1. 请确定在您的系统中安装了 Flatpak 客户端的最新版本：

```
# yum update flatpak
```

2. 启用 RHEL Flatpak 存储库：

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

3. 为 RHEL 帐户提供凭证：

```
# podman login registry.redhat.io
```

默认情况下，Podman 仅在用户没有登出前才保存凭据。

4. 可选：永久保存凭证：

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

5. 安装 Flatpak 容器镜像：

```
$ flatpak install rhel container-id
```

(JIRA:RHELPLAN-30958,  
[BZ#1920689](#),[BZ#1921179](#),[BZ#1921802](#),[BZ#1916412](#),[BZ#1921812](#),[BZ#1920604](#))

## Rust Toolset rebase 到版本 1.47.0

Rust Toolset 已更新到版本 1.47.0。主要变更包括：

- 编译时评估的功能 **const fn** 已得到改进，现在您可以使用控制流功能，例如 **if**、**while** 和 **match**。
- 新的 **#[track\_caller]** 注释现在可以放在函数上。来自注释函数的 panics 将调用者报告为源。
- Rust 标准库现在通常为任意长度的数组实现特征。在以前的版本中，只能对长度在 0 到 32 之间的数组实现 trait。

有关使用方法的详细信息，[请参阅使用 Rust Toolset](#)。

(BZ#1883839)

## 日志系统角色现在对其输出支持基于属性的过滤器

有了这个更新，基于属性的过滤器已添加到文件输出，forwards 输出和日志记录系统角色的 remote\_files 输出。该功能由底层 **rsyslog** 子角色提供，可通过日志记录 RHEL 系统角色进行配置。因此，用户可从通过属性（如主机名、标签）过滤日志消息的功能中获益，而消息本身有助于管理日志。

(BZ#1889492)

## 日志记录 RHEL 系统角色现在支持 rsyslog 行为

有了这个增强，**rsyslog** 可以接收来自 Red Hat Virtualization 的信息，并将消息转发到 **elasticsearch**。

(BZ#1889893)

## ubi8/pause 容器镜像现已可用

Podman 现在使用 **ubi8/pause** 而不是 **k8s.gcr.io/pause** 容器镜像来保存 pod 的网络命名空间信息。

(BZ#1690785)

## podman rebase 到版本 2.1

Podman 实用程序已更新至 2.1 版本。主要改进包括：

- 更改：
  - Podman 被更新至 2.2.1（从 2.0.5），Buildah 被更新至 1.19（从 1.151），Skopeo 被更新至 1.2.1（从 1.1.1），Udica 被更新至 0.2.3（从 0.2.2），CRIU 被更新至 3.15（从 0.3.4）。
  - Docker 兼容的卷 API 端点（Create、Inspect、List、Remove、Prune）现已可用
  - 添加了用于为容器生成 systemd 单元文件的 API 端点
  - **podman play kube** 命令现在支持设置容器的 CPU 和内存限制
  - **podman play kube** 命令现在支持使用 Podman 命名的卷的持久化卷声明
  - **podman play kube** 命令现在通过 **--configmap** 选项支持 Kubernetes configmaps
  - 添加了对短名称别名的实验性支持。默认情况下不启用此设置，但可以通过将环境变量 **CONTAINERS\_SHORT\_NAME\_ALIASING** 设置为 on 来启用。如需更多信息，请参阅 [Podman 中的容器镜像短名称](#)。



- 添加了新的 **podman image** 命令。这允许以只读方式挂载镜像，以检查其内容，而不必从其创建容器。
- **podman save** 和 **podman load** 命令现在可以创建和加载包含多个镜像的归档。
- 现在，如果拉取因为网络错误而失败，Podman 最多会重试拉取镜像三次。
- 程序错误修复：
  - 修复了在 cgroup v1 系统上的容器中运行 systemd 错误。

Buildah 工具已更新至 1.19 版本。主要改进包括：

- 更改：
  - **buildah inspect** 命令支持检查清单
  - **buildah push** 命令支持推送清单列表和摘要
  - 添加了对 **--manifest** 标记的支持
  - 添加了 **--arch**、**--os** 和 **--variant** 选项来选择构架和操作系统
  - 允许用户将 **stdin** 指定到容器中
  - 允许用 **--from** 选项覆盖 **FROM**
  - 添加了 **--ignorefile** 标志以使用替代的 **.dockerignore** 标志
  - 短名称别名
  - 为 **buildah pull** 命令添加了 **--policy** 选项
  - 修复了 **buildah mount** 命令以显示容器名称而不是 ID
  - 改进了 buildah 完成
  - 使用 **--timestamp** 而不是 **--omit-timestamp** 标记
  - 使用管道进行复制
  - 为 **buildah bud** 命令添加了 **--omit-timestamp** 标记
  - 为容器添加 VFS 附加镜像存储
  - 在挂载选项中，可以使用 "ro" 作为"只读"的别名
  - buildah, bud: 对并行执行支持 **--jobs=N** 选项

Skopeo 工具已更新至 1.2.1 版本。主要改进包括：

- 更改：
  - 通过 Travis 为上游和稳定的 skopeo 镜像添加多架构构建
  - 添加了对同步摘要的支持
  - 添加了 **--all** 同步标志来模拟复制 **--all**

- 为 **skopeo inspect** 命令添加了 **--format** 选项

Udica 工具已更新至 0.2.3 版本。主要改进包括：

- 更改：
  - 启用容器端口，而不是主机端口
  - 添加 **--version** 选项

CRIU 工具已更新至 3.15 版本。主要改进包括：

- 更改：
  - 初始 cgroup2 支持
  - 合法化的 swrk API 并添加了通过它继承 fds 的功能
  - 外部绑定挂载和 tasks-to-cgroups 绑定
  - **ibcriu.so**（RPC 打包程序）和插件

(JIRA:RHELPLAN-55998)

## 第 5 章 RHEL 8.3.0 发行版本

### 5.1. 新特性

本部分论述了 Red Hat Enterprise Linux 8.3 中的新特性及主要改进。

#### 5.1.1. 安装程序和镜像创建

##### Anaconda 被 rebase 到版本 33.16

在这个版本中，Anaconda 被 rebase 到版本 33.16。与上一个版本相比，这个版本提供以下显著改进。

- 安装程序现在在多行中显示静态 IPv6 地址，且不再改变窗口大小。
- 安装程序现在显示支持的 NVDIMM 设备扇区大小。
- 现在，在安装了 IPv6 静态配置的系统中配置了主机名。
- 现在您可以在磁盘加密密码短语中使用非 ASCII 字符。
- 安装程序在 /boot、/tmp 以及除 /usr/local 和 /var/www 之外的所有 /var 和 /usr 挂载点显示一个新文件系统。
- 现在，安装程序可以正确地检查键盘布局。当使用键(ALT+SHIFT) 在不同布局和语言间进行切换时，不会改变键盘布局屏幕的状态。
- 在存在 RAID1 分区的系统上，救援模式不再失败。
- 现在，在 **Manual Partitioning** 屏幕中可以更改容器的 LUKS 版本。
- 安装程序在没有 **btrfs-progs** 软件包时可以成功完成安装。
- 安装程序现在将默认 LUKS2 版本用于加密的容器。
- 当 Kickstart 文件将逻辑卷组(VG)的物理卷(PV)放置在 **ignoredisk** 列表中时，安装程序不再崩溃。
- 为系统根引进一个新的挂载路径 **/mnt/sysroot**。这个路径用来挂载目标系统的 /。通常物理根和系统根是相同的，因此 **/mnt/sysroot** 被连接到和 **/mnt/sysimage** 相同的文件系统中。唯一例外是 rpm-ostree 系统，其中的系统根更改基于部署。然后 **/mnt/sysroot** 被附加到 **/mnt/sysimage** 的子目录中。建议您使用 **/mnt/sysroot** 作为 chroot。

([BZ#1691319](#),[BZ#1679893](#), [BZ#1684045](#), [BZ#1688478](#), [BZ#1700450](#), [BZ#1720145](#), [BZ#1723888](#), [BZ#1754977](#),[BZ#1755996](#), [BZ#1784360](#), [BZ#1796310](#), [BZ#1871680](#))

#### RHEL 安装程序中的 GUI 更改

RHEL 安装程序现在在安装概述窗口中包括以下用户设置：

- root 密码
- 创建用户

在这个版本中，您可以配置 root 密码并在开始安装前创建一个用户帐户。之前，您需要在安装过程开始后配置一个 root 密码并创建用户帐户。

root 密码是用来登录管理员（又称超级用户或 root）帐户,这些帐户用于系统管理任务。用户名用于从命令行登录；如果您安装了图形环境，则图形登录管理器将使用全名。详情请参阅 [执行标准 RHEL 安装文档](#)。

(JIRA:RHELPLAN-40469)

### 镜像构建器后端 **osbuild-composer** 替换 **lorax-composer**

**osbuild-composer** 后端替换 **lorax-composer**。新服务为镜像构建提供 REST API。因此，用户可从更可靠的后端及更可预测的输出镜像中受益。

(BZ#1836211)

### 镜像构建器 **osbuild-composer** 支持一组镜像类型

借助 **osbuild-composer** 后端替换，当前 **osbuild-composer** 支持的以下镜像类型组：

- TAR Archive (.tar)
- QEMU QCOW2 (.qcow2)
- VMware Virtual Machine Disk (.vmdk)
- Amazon Machine Image (.ami)
- Azure Disk Image (.vhd)
- OpenStack Image (.qcow2)

当前不支持以下输出：

- ext4-filesystem
- partitioned-disk
- Alibaba Cloud
- Google GCE

(JIRA:RHELPLAN-42617)

### 镜像构建器 现在支持通过 GUI 推送到云

在这个版本中，在创建镜像时，用户可以通过 **GUI Image Builder** 选择推送到 **Azure** 和 **AWS** 服务云的选项。因此，用户可更容易地进行上传及安装。

(JIRA:RHELPLAN-30878)

## 5.1.2. RHEL for Edge

### RHEL for Edge 镜像

在这个版本中，您可以为 Edge 服务器创建自定义 RHEL 镜像。

您可以使用镜像构建器为 RHEL for Edge 镜像，然后使用 RHEL 安装程序在 AMD 和 Intel 64 位系统中部署它们。Image Builder 生成一个 RHEL for Edge 镜像 **rhel-edge-commit**（在一个 **.tar** 文件中）。

RHEL for Edge 镜像是一个 **rpm-ostree** 镜像，其中包含在 Edge 服务器中远程安装 RHEL 的系统软件包。

系统软件包包括：

- 基本操作系统软件包
- podman 作为容器引擎

您可以根据要求自定义镜像来配置 OS 内容，并将其部署到物理和虚拟机中。

在 RHEL for Edge 镜像中，您可以实现：

- 原子升级，每个更新的状态都是已知的，在重新引导该设备前不会看到任何变化。
- 在升级失败时，使用 Greenboot 和智能回滚进行定制健康检查。
- 以容器为主的工作流，可将核心操作系统更新与应用程序更新分开，并测试和部署不同的应用程序版本。
- 为低带宽环境优化 OTA 有效负载。
- 使用 Greenboot 自定义健康检查以确保弹性。

有关 RHEL for Edge 镜像制作、安装和管理的更多信息，请参阅 [制作、安装和管理 RHEL for Edge 镜像](#)。

(JIRA:RHELPLAN-56676)

### 5.1.3. 软件管理

#### best dnf 配置选项地默认值从 True 该为 False

有了这个更新，默认配置文件中的 **best dnf** 配置选项的值被设置为 **True**，以保留原始的 dnf 行为。因此，对于使用默认配置文件的用户来说，行为不会改变。

如果你自己提供自己的配置文件，请确定使用 **best=True** 选项来保留原有的行为。

(BZ#1832869)

#### dnf reposync 命令的新 --norepopath 选项 现在可用

在以前的版本中，**reposync** 命令默认为每个下载的仓库在 **--download-path** 目录下创建一个子目录。在这个版本中，引进了一个 **--norepopath** 选项，**reposync** 不会创建子目录。因此，仓库会直接下载到 **--download-path** 指定的目录中。YUM v3 中也有这个选项。

(BZ#1842285)

#### 启用和禁用 libdnf 插件的能力

在以前的版本中，订阅检查被写死到 **libdnf** 插件的 RHEL 版本。有了这个更新，**microdnf** 工具可以启用和禁用 **libdnf** 插件，现在可以以与 DNF 相同的方式禁用订阅检查。要禁用订阅检查，请使用 **--disableplugin=subscription-manager** 命令。要禁用所有插件，请使用 **--noplugins** 命令。

(BZ#1781126)

### 5.1.4. Shell 和命令行工具

## ReaR 更新

RHEL 8.3 对 Relax-and-Recover (**ReaR**) 工具程序引入了大量的更新。主要变更包括：

- 添加了对第三方 Rubrik Cloud Data Management(CDM)作为外部备份软件的支持。要使用它，请将配置文件中的 **BACKUP** 选项设置为 **CDM**。
- 在 IBM POWER 上创建一个大于 4 GB 的救援镜像，启用了 little endian 构架。
- 由 **ReaR** 创建的磁盘布局不再包含 Rancher 2 Longhorn iSCSI 设备和文件系统的条目。

(BZ#1743303)

## smartmontools rebase 到版本 7.1

**smartmontools** 软件包已升级至版本 7.1，提供多个程序错误修复和增强。主要变更包括：

- 在驱动器数据库中添加 HDD、SSD 和 USB。
- 启用 JSON 输出模式的新选项 **-j** 和 **--json**。
- 解决某些 SAS SSD 中不完整的 **Log** 子页面响应。
- 改进了对 **READ CAPACITY** 命令的处理。
- 日志页面解码方面的各种改进。

(BZ#1671154)

## opencryptoki rebase 到版本 3.14.0

**opencryptoki** 软件包升级至 3.14.0 版本，提供多个程序错误修复和增强。主要变更包括：

- EP11 加密服务增强：
  - 支持 Dilithium
  - Edwards-curve 数字签名算法(EdDSA)支持
  - 支持带有非 SHA1 哈希和掩码生成功能(MGF)的 Rivest-Shamir-Adleman 最佳非对称加密 padding(RSA-OAEP),
- 加强的进程和线程锁定
- 增强的 **btree** 和对象锁定
- 支持新的 IBM Z 硬件 z15
- 支持可信平台模块(TPM)、IBM 加密架构(ICA)和集成加密服务工具(ICSF)的多个令牌实例
- 添加新工具 **p11sak**，它会在 **openCryptoki** 令牌存储库中列出令牌密钥
- 添加了将令牌存储库迁移到兼容 FIPS 加密的工具
- 修复了 **pkcsep11\_migrate** 工具
- 对 ICSF 软件进行小修复

(BZ#1780293)

## gpgme 被 rebase 到版本 1.13.1。

**gpgme** 软件包已升级到上游版本 1.13.1。主要变更包括：

- 新的上下文标志 **no-symkey-cache**（与 GnuPG 2.2.7 或更高版本一起使用时起作用）、**request-origin**（与 GnuPG 2.2.6 或更新版本一起使用时起作用）、**auto-key-locate** 和 **trust-model** 已引入。
- 添加了新的工具 **gpgme-json** 作为 web 浏览器的原生 messaging 服务器。现在，支持公钥加密和解密。
- 引入了新的加密 API，以支持直接密钥规格，包括隐藏接收者选项和从文件中获取密钥。这也允许使用子密钥。

([BZ#1829822](#))

## 5.1.5. 基础架构服务

### powertop rebase 到版本 2.12

**powertop** 软件包已升级到 2.12 版本。2.11 版本的显著变化包括：

- 对 SATA 链接 PM 使用设备接口电源管理(DIPM)。
- 支持 Intel Comet Lake 移动和桌面系统、Skylake 服务器和基于 Atom 的 Tremont 架构(Jasper Lake)。

([BZ#1783110](#))

### tuned rebase 到版本 2.14.0

**tuned** 软件包已升级到上游版本 2.14.0。主要改进包括：

- 引进 **optimize-serial-console** 配置集。
- 添加了对 postload 配置集的支持。
- 添加了用于处理 **irqbalance** 设置的 **irqbalance** 插件。
- 添加了对 Marvell ThunderX 和 AMD 平台的特定架构调整。
- 调度程序插件已扩展，以支持 CPU 关联性设置的 **cgroups-v1**。

([BZ#1792264](#))

### tcpdump rebase 到版本 4.9.3

**tcpdump** 工具已更新至版本 4.9.3，以修复常见漏洞和风险(CVE)。

([BZ#1804063](#))

### libpcap rebase 到版本 1.9.1

**libpcap** 软件包已更新至版本 1.9.1，以修复常见漏洞和风险(CVE)。

([BZ#1806422](#))

**iperf3** 现在在客户端支持 **sctp** 选项

有了这个增强，用户可以在测试网络吞吐量的客户端使用流控制传输协议(SCTP)而不是传输控制协议(TCP)。

以下 **iperf3** 的选项现在包括在测试的客户端中：

- **--sctp**
- **--xbind**
- **--nstreams**

要获得更多信息，请参阅 **iperf3** man 页中的 **Client Specific Options**。

(BZ#1665142)

### **iperf3 现在支持 SSL**

有了这个增强，用户可以在客户端和服务端之间使用 RSA 身份验证，将到服务器的连接限制为合法客户端。

现在，在服务器端支持 **iperf3** 的以下选项：

- **--rsa-private-key-path**
- **--authorized-users-path**

以下 **iperf3** 的选项现在包括在客户端：

- **--username**
- **--rsa-public-key-path**

(BZ#1700497)

### **bind rebase 到 9.11.20**

**bind** 软件包已升级到版本 9.11.20，它提供了多个 bug 修复和增强。主要变更包括：

- 通过修复多个竞争条件，提高有很多 CPU 内核的系统的可靠性。
- 详细错误报告：**dig** 和其它工具现在可以打印扩展 DNS 错误(EDE)选项。
- 当入站 DNS 区域传输协议(AXFR)中的消息 ID 不一致时，会对其进行检查和记录。

(BZ#1818785)

### **增加了一个新的 optimize-serial-console TuneD 配置集，通过降低 printk 值来减小到串口控制台的 I/O**

在这个版本中，包括了一个新的 **optimize-serial-console** TuneD 配置集。在某些情况下，内核驱动程序可将大量 I/O 操作发送到串口控制台。在将 I/O 写入串口控制台时，这种行为可能会导致系统临时无响应。**optimize-serial-console** 配置集通过把 **printk** 的值从默认的 **7 4 1 7** 改为 **4 4 1 7** 来减少了这类 I/O 具有串行控制台的用户如果希望在自己的系统中进行此更改，则可按如下方式检测其系统：

```
# tuned-adm profile throughput-performance optimize-serial-console
```

因此，用户在重启后会得到一个较小的 **printk** 值，这降低了系统停滞的可能性。



这个 TuneD 配置集删除了调试信息，从而减少了写入串口控制台的 I/O 数量。如果您需要收集这个调试信息，应该确保未启用此配置集，并将您的 `printk` 值设为 `7 4 1 7`。检查 `printk run` 的值：

```
# cat /proc/sys/kernel/printk
```

([BZ#1840689](#))

### 为基于 AMD 的平台添加新的 TuneD 配置集

在 RHEL 8.3 中，**throughput-performance** TuneD 配置集被更新为包括基于 AMD 的平台性能优化。不需要手动更改任何参数，它会在 AMD 系统中自动应用调整。**AMD Epyc Naples** 和 **Rome** 系统在默认的 **throughput-performance** 配置集中修改以下参数：

**sched\_migration\_cost\_ns=5000000** 和 **kernel.numa\_balancing=0**

通过这个变化，系统性能大约提高了 5%。

([BZ#1746957](#))

### memcached rebase 到版本 1.5.22

**memcached** 软件包已升级至 1.5.22 版本。与以前版本相比的显著变化包括：

- 启用 TLS。
- 删除 `-o inline_ascii_response` 选项。
- 添加 `-Y [authfile]` 选项和 ASCII 协议的验证模式。
- **Memcached** 现在可以在重启之间恢复缓存。
- 添加了新的实验性 `meta` 命令。
- 各种性能改进。

([BZ#1809536](#))

## 5.1.6. 安全性

### Cyrus SASL 现在支持使用 SASL/GSSAPI 和 SASL/GSS-SPNEGO 插件的通道绑定

在这个版本中增加了对 **SASL/GSSAPI** 和 **SASL/GSS-SPNEGO** 插件的通道绑定的支持。因此，当在 **openldap** 库中使用时，此功能使 **Cyrus SASL** 能够保持与 Microsoft Active Directory 和 Microsoft Windows 系统的兼容性和访问权限，它们为 LDAP 连接引入了强制通道绑定。

([BZ#1817054](#))

### Libreswan rebase 到 3.32

在这个版本中，**Libreswan** 基于上游版本 3.32，其中包括几个新功能和程序错误修复。主要特性包括：

- **libreswan** 不再需要独立的 FIPS 140-2 认证。
- **libreswan** 现在实现了 RFC 8247 的加密建议，并将首选从 SHA-1 和 RSA-PKCS v1.5 改为 SHA-2 和 RSA-PS。
- **libreswan** 支持 XFRMi 虚拟 `ipsecXX` 接口来简化编写防火墙规则的过程。

- 改进了在完整加密网络中恢复崩溃和重新引导节点的过程。

([BZ#1820206](#))

### libssh 程序库已更新至 0.9.4 版本

使用 SSH 协议的 **libssh** 库已升级至 0.9.4 版本。

此更新包括程序错误修正和增强,其中包括：

- 添加了对 PEM 文件中 **Ed25519** 密钥的支持。
- 添加了对 **diffie-hellman-group14-sha256** 密钥交换算法的支持。
- 添加了对 **libssh** 客户端配置文件中 **Match** 关键字中 **localuser** 的支持。
- **Match** 条件关键字参数现在区分大小写（请注意，关键字区分大小写，但关键字参数区分大小写）
- 修复了 CVE-2019-14889 和 CVE-2020-1730。
- 添加了递归创建已知主机文件提供的路径字符串中缺失的目录的支持。
- 添加了对 PEM 文件中带有注释和头空白的 **OpenSSH** 密钥的支持。
- 从 **libssh** 服务器配置中删除了 **OpenSSH** 服务器配置中包含的 OpenSSH 服务器配置。

([BZ#1804797](#))

### gnutls rebase 到 3.6.14

**gnutls** 软件包已更新至上游版本 3.6.14。这个版本提供很多程序错误的修正和增强，最重要的是：

- **gnutls** 现在拒绝包含无效字符或格式的 **Time** 字段的证书。
- **gnutls** 现在检查可信 CA 证书以最小密钥大小。。
- 显示加密的私钥时，**certtool** 工具不再包含其纯文本描述。
- 使用 **gnutls** 的服务器现在宣传对 OCSP 交换的支持。
- 使用 **gnutls** 的客户端现在只根据请求发送 OCSP 错误。

([BZ#1789392](#))

### gnutls FIPS DH 检查现在与 NIST SP 800-56A rev 一致。3

这个对 **gnutls** 软件包的更新提供了 NIST Special Publication 800-56A Revision 3，第 5.7.1.1 和 5.7.1.2 节，第 2 步所需的检查。对于将来的 FIPS 140-2 认证，需要进行修改。因此，在以 FIPS 模式操作时，在 Diffie-Hellman 密钥交换过程中，**gnutls** 现在只接受 2048 位或来自 RFC 7919 和 RFC 3526 的更大的参数。

([BZ#1849079](#))

### gnutls 现在根据 NIST SP 800-56A rev 3 执行验证

这个对 **gnutls** 软件包的更新添加了 NIST Special Publication 800-56A Revision 3，第 5.6.2.2.2 和 5.6.2.1.3 节，第 2 步所需的检查。这为将来的 FIPS 140-2 认证进行准备 **gnutls**。因此，在使用 FIPS 模式操作时，**gnutls** 在 Diffie-Hellman 密钥交换过程中为生成和接收的公钥执行额外的验证步骤。

(BZ#1855803)

### update-crypto-policies 和 fips-mode-setup 移动到 crypto-policies-scripts 中

**update-crypto-policies** 和 **fips-mode-setup** 脚本以前包括在 **crypto-policies** 软件包中，现在它们被移到一个单独的 RPM 软件包 **crypto-policies-scripts** 中。软件包通过推荐对常规安装的依赖关系自动安装。这可让 **ubi8/ubi-minimal** 镜像避免出现 Python 语言解释器，从而减少镜像大小。

(BZ#1832743)

### OpenSC rebase 到版本 0.20.0

**opensc** 软件包已更新为 0.20.0 版本，它解决了多个程序错误和安全问题。主要变更包括：

- 在这个版本中，**CVE-2019-6502**、**CVE-2019-15946**、**CVE-2019-15945**、**CVE-2019-19480**、**CVE-2019-19481** 和 **CVE-2019-19479** 安全问题已被解决。
- OpenSC 模块现在支持 **C\_WrapKey** 和 **C\_UnwrapKey** 功能。
- 您现在可以按预期使用工具检测插入和移除卡片读取器。
- **pkcs11-tool** 程序现在支持 **CKA\_ALLOWED\_MECHANISMS** 属性。
- 这个版本允许默认检测 **OsEID** 卡。
- OpenPGP 卡 v3 现在支持 **Elliptic Curve Curve Cryptography (ECC)**。
- PKCS#11 URI 现在使用 **ellipsis** 截断读者名称。

(BZ#1810660)

### stunnel 被 rebase 到版本 5.56

在这个版本中，**stunnel** 加密打包程序更新到上游社区版本 5.56，其中包括几个新功能和程序错误修复。主要特性包括：

- 新的 **ticketKeySecret** 和 **ticketMacSecret** 选项，控制所发出会话问题单的机密性和完整性保护。这些选项允许您恢复集群中其他节点的会话。
- 新的 **curves** 选项控制 OpenSSL 1.1.0 及之后的版本中的 elliptic curves 列表。
- 新的 **ciphersuites** 选项来控制允许的 TLS 1.3 密码组列表。
- 为 OpenSSL 1.1.0 及之后的版本添加了 **sslVersion**、**sslVersionMin** 和 **sslVersionMax**

(BZ#1808365)

### libkcapi rebased 到版本 1.2.0

**libkcapi** 软件包更新到上游版本 1.2.0，它包括了较小的修改。

(BZ#1683123)

### setools rebase 到版本 4.3.0

**setools** 软件包是设计用于进行 SELinux 策略分析的工具集合，已升级到 4.3.0 版本。

此更新包括程序错误修正和增强,其中包括：

- 修订了 Type Enforcing(TE)规则的 **sediff** 方法，这可显著减少内存和运行时问题。
- 为 **seinfo**、**sediff** 和 **apol** 增加了 **infiniband** 上下文支持
- 添加了用于显示在线文档的 Qt 工具程序位置的 **apol** 配置。
- 修复了以下 **sediff** 问题：
  - 如果没有请求，显示属性标头。
  - **type\_transition** 文件的名称对比。
- 修复了 map socket **sendto** 信息流方向的权限问题。
- 在 **TypeAttribute** 类中添加了方法使其成为完整的 Python 集合。
- **Genfscon** 现在会查找类，而不是使用从 **libsepol** 中丢出的固定值。

**setools** 软件包需要以下软件包：

- **setools-console**
- **setools-console-analyses**
- **setools-gui**

([BZ#1820079](#))

### 单个 CephFS 文件和目录现在可以有 SELinux 标签

Ceph 文件系统(CephFS)最近启用了在文件的扩展属性中存储 SELinux 标签。在以前的版本中，CephFS 卷中的所有文件都有一个通用标签 **system\_u:object\_r:cephfs\_t:s0**。在这个改进中，您可以更改单个文件的标签，SELinux 根据过渡规则定义新创建的文件标签。请注意，之前未标记的文件仍旧有 **system\_u:object\_r:cephfs\_t:s0** 标签，直到显式更改为止。

([BZ#1823764](#))

### OpenSCAP rebase 到版本 1.3.3

**openscap** 软件包已升级到上游版本 1.3.3，与之前的版本相比它提供了很多 bug 修复和增强，最重要的是：

- 添加了 **autotailor** 脚本，可让您使用命令行界面(CLI)生成量身定做的文件。
- 向可扩展的配置清单描述格式(XCCDF)TestResult 启动和结束时间戳添加了时区部分
- 添加 **yamfilecontent** 独立探测作为实施草稿。
- 在 XCCDF 中引入了 **urn:xccdf:fix:script:kubernetes** 修复类型。
- 添加了生成 **machineconfig** 修复的功能。
- **oscap-podman** 工具现在可以检测模糊的扫描目标。
- **rpmverifyfile** 探测现在可以从 **/bin** 目录中验证文件。
- 修复了在 **textfilecontent58** 探测中执行复杂常规表达式时的崩溃问题。
- XCCDF 报告的评估特性现在与 **system\_info** 探测中的 OVAL 实体一致。

- 修复了 `textfilecontent58` 探测中离线模式下文件路径模式匹配。
- 修复了 `systemdunitdependency` 探测中的无限重复的问题。

([BZ#1829761](#))

### SCAP 安全指南现在提供了一个与 CIS RHEL 8 Benchmark v1.0.0 一致的配置集。

在这个版本中, `scap-security-guide` 软件包提供了一个与 CIS Red Hat Enterprise Linux 8 Benchmark v1.0.0 一致的配置集。这个配置可让您使用互联网安全中心(CIS)提供的指南强化系统配置。因此, 您可以使用 CIS Ansible Playbook 和 CIS SCAP 配置集配置并自动化 RHEL 8 系统与 CIS 的合规性。

请注意, CIS 配置集中的 `rpm_verify_permissions` 规则无法正常工作。

([BZ#1760734](#))

### `scap-security-guide` 现在提供了一个可以实现 HIPAA 的配置集

这个 `scap-security-guide` 软件包更新在 RHEL 8 安全合规内容中增加了 Health Insurance Portability and Accountability Act (HIPAA) 配置集。此配置集实施 [HIPAA 隐私规则](#) 网站上的建议。

HIPAA 安全规则建立了美国国家标准, 以保护由涉及的实体创建、接收、使用或维护的个人电子健康信息。安全规则要求适当的管理、物理和技术保护, 以确保电子保护的健康信息的机密性、完整性和安全性。

([BZ#1832760](#))

### `scap-security-guide` rebase 到 0.1.50

`scap-security-guide` 软件包 (包含 Linux 系统的最新安全策略集合) 已升级至版本 0.1.50。

这个版本包括程序错误修正和增强, 最重要的是 :

- Ansible 内容已被改进 : 第一次有多个包含 Ansible 补救的规则, 其他规则已更新, 以解决程序错误修复。
- 修正并改进 `scap-security-guide` 内容以扫描 RHEL7 系统, 包括 :
  - `scap-security-guide` 软件包现在提供与 CIS RHEL 7 Benchmark v2.2.0 一致的配置集。请注意, CIS 配置集中的 `rpm_verify_permissions` 规则无法正常工作。在 [CIS 配置文件中](#), `rpm_verify_permissions` 失败是一个已知的问题。
  - SCAP 安全指南配置集现在可以正确地禁用和屏蔽不应启动的服务。
  - `scap-security-guide` 软件包中的 `audit_rules_privileged_commands` 规则现在可以在特权命令中正常工作。
  - 对 `scap-security-guide` 软件包中的 `dconf_gnome_login_banner_text` 规则的修正不再会失败。

([BZ#1815007](#))

### SCAP Workbench 现在可以根据定制的配置集生成基于结果的补救方法。

在这个版本中, 您可以使用 `SCAP Workbench` 工具从定制的配置集生成基于结果的补救角色。

([BZ#1640715](#))

### 新的 Ansible 角色提供 Clevis 客户端的自动部署

这个 **rhel-system-roles** 软件包的更新引入了 **nbde\_client** RHEL 系统角色。这个 Ansible 角色允许您自动部署多个 Clevis 客户端。

([BZ#1716040](#))

### 新的 Ansible 角色现在可以设置 Tang 服务器

在这个改进中，您可以使用新的 **nbde\_server** 系统角色部署和管理 Tang 服务器作为自动磁盘加密解决方案的一部分。**nbde\_server** Ansible 角色包含在 **rhel-system-roles** 软件包中，它支持以下功能：

- 轮转 Tang 密钥
- 部署和备份 Tang 密钥

如需更多信息，请参阅 [轮转 Tang 服务器密钥](#)。

([BZ#1716039](#))

### clevis rebase 到版本 13

**clevis** 软件包升级至版本 13，提供多个程序错误修复和增强。主要变更包括：

- **clevis luks unlock** 可在设备中使用非互动模式的密钥文件。
- 如果输入以 JSON 阵列形式提供，**clevis encrypt tpm2** 会解析 **pcr\_ids** 项。
- **clevis-luks-unbind(1)** 手册页不再只引用 LUKS v1。
- 如果给定的密码不正确，**clevis luks bind** 不会再写入非活动的插槽。
- 当系统使用非英语区域时，**clevis luks bind** 现在可以正常工作。
- 添加了对 **tpm2-tools** 4.x 的支持。

([BZ#1818780](#))

### Clevis luks edit 可让您编辑特定的 pin 配置

这个 **clevis** 软件包更新引进了新的 **clevis luks edit** 子命令，可让您编辑特定的 pin 配置。例如，您现在可以更改 Tang 服务器的 URL 地址和 TPM2 配置中的 **pcr\_ids** 参数。您还可以添加和删除新 **sss** pin 并更改 **sss** pin 的阈值。

([BZ#1436735](#))

### clevis luks bind -y 现在允许自动绑定

在这个版本中，Clevis 支持使用 **-y** 参数自动绑定。现在，可以将 **-y** 选项与 **clevis luks bind** 命令一同使用，该命令可使用 **yes** 自动回答后续提示。例如，在使用 Tang pin 时，您不再需要手动信任 Tang 密钥。

([BZ#1819767](#))

### fapolicyd rebase 为版本 1.0

**fapolicyd** 软件包已改为版本 1.0，它提供多个程序错误修复和增强。主要变更包括：

- 已解决多个线程同步问题。
- 通过减少数据库的大小和载入时间来提高性能。

- 为 **fapolicyd.conf** 文件中的 **fapolicyd** 软件包增加了一个新的信任选项，以自定义信任后端。您可以将所有可信文件、二进制文件和脚本添加到新的 **/etc/fapolicyd/fapolicyd.trust** 文件中。
- 您可以使用 CLI 管理 **fapolicyd.trust** 文件。
- 您可以使用 CLI 清理或转储数据库。
- **fapolicyd** 软件包会覆盖 magic 数据库来更好地解码脚本。根据覆盖，CLI 会输出类似文件命令的 MIME 类型。
- **/etc/fapolicyd/fapolicyd.rules** 文件支持使用一组值作为属性值。
- **fapolicyd** 守护进程有一个 **syslog\_format** 选项，用于设置 **audit/syslog** 事件格式。

(BZ#1817413)

### fapolicyd 现在在 fapolicyd-selinux 中提供自己的 SELinux 策略

在这个版本中，**fapolicyd** 框架提供了自己的 SELinux 安全策略。守护进程被限制在 **fapolicyd\_t** 域下，并通过 **fapolicyd-selinux** 子软件包安装该策略。

(BZ#1714529)

### USBGuard rebase 到版本 0.7.8

**usbguard** 软件包被更新到版本 0.7.8，它提供多个程序错误修复和增强。主要变更包括：

- **/etc/usbguard/usbguard-daemon.conf** 文件中的 **HidePII=true|false** 参数现在可以隐藏审计条目中的个人可识别信息。
- **/etc/usbguard/usbguard-daemon.conf** 文件中的 **AuthorizedDefault=keep|none|all|internal** 参数可预定义控制器设备的授权状态。
- 使用新的 **withconnect-type** 规则属性，用户现在可以区分设备的连接类型。
- 用户现在可以使用 **-t** 选项添加临时规则。在守护进程重启前，临时规则都会保留在内存中。
- **usbguard list-rules** 现在可以根据特定属性过滤规则。
- **usbguard generate-policy** 现在可以为特定设备生成策略。
- **usbguard allow|block|reject** 命令现在可以处理规则字符串，并在每个与指定规则字符串匹配的设备上都应用一个目标。
- 包括了新的子软件包 **usbguard-notifier** 和 **usbguard-selinux**。

(BZ#1738590)

### USBGuard 为企业桌面用户提供很多改进

这个对 USBGuard 项目的增加包含了增强和 bug 修复，以提高企业桌面用户的可用性。主要变更包括：

- 为了保持 **/etc/usbguard/rules.conf** 规则文件的完整性，用户可以在 **RuleFolder=/etc/usbguard/rules.d/** 目录里定义多个配置文件。默认情况下，**RuleFolder** 在 **/etc/usbguard-daemon.conf** 文件中指定。
- **usbguard-notifier** 工具现在提供 GUI 通知。工具会在设备被插入或被拔出时、以及设备是否被任何用户允许、阻塞或拒绝时通知用户。

- 现在您可以在配置文件中包括注释，**usbguard-daemon** 不再解析以 **#** 开始的行。

(BZ#1667395)

### USBGuard 现在在 **usbguard-selinux** 中提供自己的 SELinux 策略

在这个版本中，USBGuard 框架提供了自己的 SELinux 安全策略。该守护进程限制在 **usbguard\_t** 域下，并通过 **usbguard-selinux** 子软件包安装该策略。

(BZ#1683567)

### libcap 现在支持不同的能力

在这个版本中，用户可以在登录时授予不固定的功能，并避免具有适当配置的进程的 root 访问权限。

(BZ#1487388)

### libseccomp 库已更新到 2.4.3 版本

libseccomp 库为 seccomp 系统调用过滤机制提供了一个界面，它已升级到 2.4.3 版本。

这个版本提供了大量的程序错误修正和增强。主要变更包括：

- 更新了 Linux v5.4-rc4 的 **syscall** 表。
- 不再为不存在的系统调用定义 **\_\_NR\_x** 值。
- **\_\_SNR\_x** 现在内部使用。
- 为 **\_\_SNR\_ppoll** 增加了 **define**。
- 修复了 s390/s390x shm\* 系统调用的问题。
- 从 libseccomp 工具编译中删除了 **static** 标志。
- 添加了对 **io-uring** 相关系统调用的支持。
- 修复了 v2.4.0 发行版中引入的 Python 模块命名问题；与之前一样，该模块被命名为 **seccomp**。
- 修复了 **clang** 在 **scmp\_bpf\_sim** 工具中识别的潜在内存泄漏。

(BZ#1770693)

### omamqp1 模块现在被支持

有了这个版本更新，**AMQP 1.0** 协议支持将消息发送到总线上的目的地。在以前的版本中，Openstack 使用 **AMQP1** 协议作为通信标准，此协议现在可以在 AMQP 信息中记录信息。这个更新引进了 **rsyslog-omamqp1** 子软件包，来交付 **omamqp1** 输出模式，它会记录消息并将其发送到总线上的目的地。

(BZ#1713427)

### OpenSCAP 压缩远程内容

有了这个更新，OpenSCAP 使用 **gzip** 压缩来传输远程内容。最常见的远程内容类型是基于文本的 CVE 提要，其大小随着时间的推移而增加，通常每次扫描都必须下载。**gzip** 压缩将带宽降至未压缩内容所需带宽的 10%。因此，这就降低了扫描系统和托管远程内容的服务器之间的整个链的带宽要求。

(BZ#1855708)



## SCAP 安全指南现在提供了一个与 NIST-800-171 一致的配置集

有了这个更新，**scap-security-guide** 软件包提供了一个与 NIST-800-171 标准一致的配置文件。该配置文件使您能够根据非联邦信息系统中受控的未机密信息(CUI)的安全要求来强化系统配置。因此，您可以更轻松配置系统，使其与 NIST-800-171 标准一致。

([BZ#1762962](#))

### 5.1.7. 网络

#### IPv4 和 IPv6 连接跟踪模块已合并到 `nf_conntrack` 模块

这个功能将 `nf_conntrack_ipv4` 和 `nf_conntrack_ipv6` Netfilter 连接跟踪模块合并到 `nf_conntrack` 内核模块中。由于这个变化，将特定于地址系列的模块列入黑名单不再适用于 RHEL 8.3，您只能将 `nf_conntrack` 模块列入黑名单，以禁用对 IPv4 和 IPv6 协议的连接跟踪支持。

([BZ#1822085](#))

#### firewalld 升级到版本 0.8.2

**firewalld** 软件包已升级到上游版本 0.8.2，它修复了几个程序错误。详情请查看 [firewalld 0.8.2 发行注记](#)。

([BZ#1809636](#))

#### NetworkManager rebase 到版本 1.26.0

**NetworkManager** 软件包升级至上游版本 1.26.0，它提供了大量的改进和程序错误修复：

- NetworkManager 在停用设备时将自动协商、速度和双工设置重置为原始值。
- 现在，如果所有之前的激活尝试失败，Wi-Fi 配置集会自动连接。这意味着，初始无法自动连接到网络不再阻断自动性能。副作用是之前阻断的现有 Wi-Fi 配置集会自动连接。
- 添加了 `nm-settings-nmcli(5)` 和 `nm-settings-dbus(5)` man page。
- 添加了对多个网桥参数的支持。
- 添加了对虚拟路由和转发（VRF）接口的支持。详情请查看 [在不同的接口上永久重复使用相同的 IP 地址](#)。
- 添加了对 Wi-Fi 网络的 Opportunistic Wireless Encryption（OWE）模式的支持。
- NetworkManager 现在根据 [RFC 3021](#) 支持 IPv4 点对点链接上的 31 位前缀。
- `nmcli` 工具现在支持使用 `nmcli connection modify <connection_name> remove <setting>` 命令删除设置。
- 如果缺少主设备，NetworkManager 不再创建并激活从设备。

如需了解更多与显著变化相关的信息，请参阅上游发行注记：

- [NetworkManager 1.26.0](#)
- [NetworkManager 1.24.0](#)

([BZ#1814746](#))

## XDP 被有条件地支持

只有满足以下条件时，红帽才支持 eXpress Data Path (XDP) 功能：

- 您在 AMD 或者 Intel 64 位构架中载入 XDP 程序
- 您可以使用 **libxdp** 库将程序加载到内核中
- XDP 程序使用以下返回代码之一：**XDP\_ABORTED**、**XDP\_DROP** 或 **XDP\_PASS**
- XDP 程序不使用 XDP 硬件卸载

有关不支持的 XDP 特性的详情，请查看 [以技术预览形式提供的 XDP 特性的概述](#)

(BZ#1889736)

## 部分支持 xdp-tools

现在，AMD 和 Intel 64 位构架支持 **xdp-tools** 软件包，其包含内核 eXpress Data Path(XDP)功能的用户空间支持工具。这包括 **libxdp** 库、用于加载 XDP 程序的 **xdp-loader** 工具，以及用于数据包过滤的 **xdp-filter** 示例程序。请注意，从启用了 XDP 的网络接口捕获数据包的 **xdpdump** 工具还是一个技术预览。(BZ#1820670)

## dracut 工具默认在初始 RAM 磁盘中使用 NetworkManager

在以前的版本中，**dracut** 程序使用 shell 脚本管理初始 RAM 磁盘 **initrd** 中的网络功能。在某些情况下，这可能会造成问题。例如，NetworkManager 会发送另一个 DHCP 请求，即使 RAM 磁盘中的脚本已经请求了一个 IP 地址，这可能导致超时。

在这个版本中，**dracut** 在初始 RAM 磁盘中使用 NetworkManager，并防止系统运行时出现问题。如果您想要切回到以前的实现，并重新创建 RAM 磁盘镜像，请使用以下命令：

```
# echo 'add_dracutmodules+=" network-legacy "' > /etc/dracut.conf.d/enable-network-legacy.conf
# dracut -vf --regenerate-all
```

(BZ#1626348)

## 内核命令行中的网络配置已整合到 ip 参数下

在内核命令行中设置网络配置的 **ipv6**、**netmask**、**gateway** 和 **hostname** 参数已整合到 **ip** 参数下。**ip** 参数接受不同的格式，如下所示：

```
ip=__IP_address__:__peer__:__gateway_IP_address__:__net_mask__:__host_name__:__interface_name__:__configuration_method__
```

有关此参数接受的各个字段以及其他格式的详情，请查看 **dracut.cmdline(7)** 手册页中 **ip** 参数的描述。

RHEL 8 中不再提供 **ipv6**、**netmask**、**gateway** 和 **hostname** 参数。

(BZ#1905138)

## 5.1.8. 内核

### RHEL 8.3 中的内核版本

Red Hat Enterprise Linux 8.3 带有内核版本 4.18.0 240。

[\(BZ#1839151\)](#)

## RHEL 8.3 的扩展 Berkeley Packet 过滤器

**Extended Berkeley Packet Filter (eBPF)** 是一个内核中的虚拟机,允许在可访问有限功能的受限沙箱环境中在内核空间中执行代码。虚拟机执行类特殊的装配代码。

**eBPF** 字节码首先加载到内核, 然后进行验证, 通过即时编译到原生物理代码转换, 然后虚拟机执行代码。

红帽提供大量使用 **eBPF** 虚拟机的组件。每个组件处于不同的开发阶段, 因此目前并不完全支持所有组件。在 RHEL 8.3 中, 支持以下 **eBPF** 组件:

- **The BPF Compiler Collection (BCC)** 工具软件包, 提供用于使用 **eBPF** 的 I/O 分析、联网和监控 Linux 操作系统的工具
- **BCC** 库, 它允许开发与 **BCC** 工具软件包中相似的工具。
- **eBPF for Traffic Control (tc)** 功能, 可在内核网络数据路径中启用可编程数据包处理。
- **eXpress Data Path (XDP)** 功能在内核网络堆栈处理它们前提供对接收的数据包的访问, 在特定情况下被支持。详情请参考发行注记的 [Networking](#) 部分。
- **libbpf** 软件包对于 bpf 相关应用程序 (如 **bpftrace** 和 **bpf/xdp** 开发) 至关重要。如需了解更多详细信息, 请参阅[完全支持的专用发行注记 libbpf](#)。
- 包含 **XDP** 功能的用户空间支持工具的 **xdp-tools** 软件包, 现在在 AMD 和 Intel 64 位构架上受支持。这包括 **libxdp** 库、用于加载 XDP 程序的 **xdp-loader** 工具以及用于数据包过滤的 **xdp-filter** 示例程序。请注意, 用于从启用了 XDP 的网络接口捕获数据包的 **xdpdump** 工具仍是一个不受支持的技术预览。如需了解更多详细信息, 请参阅发行注记的 [Networking](#) 部分。

请注意, 所有其他 **eBPF** 组件都作为技术预览提供, 除非有特定的组件被显示为受支持。

以下显著的 **eBPF** 组件当前作为技术预览提供:

- **bpftrace** 追踪语言
- 用于连接 **eXpress Data Path (XDP)** 路径到用户空间的 **AF\_XDP** 套接字

如需有关技术预览组件的更多信息, 请参阅[技术预览](#)。

[\(BZ#1780124\)](#)

## Cornelis 网络 Omni-Path 架构(OPA)主机软件

Red Hat Enterprise Linux 8.3 完全支持 Omni-Path Architecture (OPA) 主机软件。OPA 为在集群环境中的计算和 I/O 节点之间的高性能数据传输 (高带宽、高消息率、低延迟) 提供主机 Fabric Interface (HFI) 硬件初始化和设置。

[\(BZ#1893174\)](#)

## 现在默认禁用 TSX

从 RHEL 8.3 开始, 内核会默认禁用 Intel® Transactional Synchronization Extensions (**TSX**) 技术以提高 OS 的安全性。此更改适用于支持禁用 **TSX** 的 CPU, 包括第二代 Intel® Xeon® Scalable Processors (以前被称为 Cascade Lake with Intel® C620 Series Chipsets)。

对于其应用程序不使用 **TSX** 的用户, 该更改消除了第二代 Intel® Xeon® Scalable Processors 上 **TSX Asynchronous Abort (TAA)** 缓解措施的默认的性能损失。

此更改还使 RHEL 内核行为与上游一致。上游自 Linux 5.4 开始默认禁用 **TSX**。

要启用 **TSX**，请在内核命令行中添加 **tsx=on** 参数。

(BZ#1828642)

## RHEL 8.3 现在支持页面所有者跟踪功能

在这个版本中，您可以使用页面所有者跟踪功能来观察内存在页面分配级别的使用情况。

要启用页面跟踪程序，请执行以下步骤：

```
# grubby --args="page_owner=on" --update-kernel=0
# reboot
```

页面所有者跟踪会跟踪内核内存消耗情况，这有助于调试内核内存泄漏并检测使用大量内存的驱动程序。

(BZ#1825414)

## 现在支持 EDAC for AMD EPYC™ 7003 系列处理器

此增强为 AMD EPYC™ 7003 系列处理器提供了错误检测和修正(EDAC)设备支持。在以前的版本中，修正的(CE)和未修正(UE)内存错误不会在基于 AMD EPYC™ 7003 系列处理器的系统上报告。在这个版本中，会使用 EDAC 来报告这些错误。

(BZ#1735611)

## Flamegraph 支持 perf 工具

在这个版本中，**perf** 命令行工具支持 flamegraphs 来生成系统性能的图形化表示。**perf** 数据被分组成带有类似堆栈后端的样本。因此，这些数据被转换为可视化表示，以便更容易地识别计算密集型代码区域。要使用 **perf** 工具生成 flamegraph，请执行以下命令：

```
$ perf script record flamegraph -F 99 -g -- stress --cpu 1 --vm-bytes 128M --timeout 10s
stress: info: [4461] dispatching hogs: 1 cpu, 0 io, 0 vm, 0 hdd
stress: info: [4461] successful run completed in 10s
[ perf record: Woken up 1 times to write data ]
[ perf record: Captured and wrote 0.060 MB perf.data (970 samples) ]
$ perf script report flamegraph
dumping data to flamegraph.html
```

注：要生成 flamegraphs，请安装 **js-d3-flame-graph** rpm。

(BZ#1281843)

## /dev/random 和 /dev/urandom 现在由 Kernel Crypto API DRBG 有条件地开机

在 FIPS 模式中，**/dev/random** 和 **/dev/urandom** 伪随机数生成器由 Kernel Crypto API Deterministic Random Bit Generator(DRBG)提供支持。FIPS 模式中的应用程序使用上述设备作为 FIPS 兼容的 noise 源，因此设备必须使用 FIPS 批准的算法。为了达到这个目的，需要在 **/dev/random** 驱动中添加了必需的 hook。因此，hook 在 FIPS 模式中被启用，并导致 **/dev/random** 和 **/dev/urandom** 连接到 Kernel Crypto API DRBG。

(BZ#1785660)

## libbpf 完全支持

现在，完全支持 **libbpf** 软件包，它对于 **bpftrace** 和 **bpf/xdp** 开发很重要。

它是 bpf-next linux tree **bpf-next/tools/lib/bpf** 目录及其支持的标题文件镜像。软件包的版本反映了应用程序二进制接口(ABI)的版本。

(BZ#1759154)

### Ishw 工具现在提供额外的 CPU 信息

在这个改进中, List Hardware utility (*Ishw*) 会显示更多 CPU 信息。CPU **version** 项现在以数字格式提供系统处理器的家族、模型和步骤, 格式为 **version: <family>.<model>.<stepping>**

(BZ#1794049)

### kernel-rt 源树已更新至 RHEL 8.3 树

**kernel-rt** 源已更新为使用最新的 Red Hat Enterprise Linux 内核源树。实时补丁集也更新至最新的上游版本 v5.6.14-rt7。这两个更新都提供很多程序错误修正和增强。

(BZ#1818138, BZ#1818142)

### tpm2-tools rebase 到版本 4.1.1

**tpm2-tools** 软件包已升级至版本 4.1.1, 其提供了大量命令添加、更新和删除。如需了解更多详细信息, 请参阅 [在 RHEL8.3 中更新到 tpm2-tools 软件包](#) 解决方案。

(BZ#1789682)

### Mellanox ConnectX-6 Dx 网络适配器现已获得全面支持

在这个版本中, Mellanox ConnectX-6 Dx 网络适配器的 PCI ID 被添加到 **mlx5\_core** 驱动中。在使用这个适配器的主机上, RHEL 会自动加载 **mlx5\_core** 驱动程序。此功能以前作为技术预览提供, 现在在 RHEL 8.3 中被完全支持。

(BZ#1782831)

### mlxsw 驱动程序 rebase 到版本 5.7

**mlxsw 驱动程序** 升级至上游版本 5.7, 包括以下新功能:

- 共享缓冲区占用功能, 其提供缓冲区占用数据。
- 数据包丢弃功能, 其启用监控 **第 2 层、第 3 层、隧道** 和 **访问控制列表** 丢弃。
- 支持数据包抓取策略器。
- 默认端口优先级配置支持使用链路层发现协议(LLDP)代理。
- 增强的传输选择(ETS)和令牌桶过滤器(TBF)排队规则卸载支持。
- 启用了 RED 排队规则 **nodrop** 模式, 以防止早期数据包丢失。
- 流量类 SKB 编辑操作 **skbedit** 优先级功能允许更改数据包元数据, 并且使用 **pedit** 流量类卸载 (TOS)进行补充。

(BZ#1821646)

### 崩溃内核现在为 kdump 扩展内存保留

有了这个增强, **crashkernel=auto** 参数会在具有 4GB 内存到 64GB 内存容量的机器上保留更多的内存。在以前的版本中, 由于内存保留的有限, 随着内核空间和用户空间内存的扩展, 崩溃内核无法捕获崩溃转

储。因此，崩溃内核会出现内存不足(OOM)错误。这个更新有助于减少上述场景中 OOM 错误的发生，并为 **kdump** 相应地扩展内存容量。

(BZ#1746644)

## 5.1.9. 文件系统和存储

### LVM 现在可以管理 VDO 卷

LVM 现在支持 Virtual DataOptimizer(VDO)片段类型。现在，您可以使用 LVM 工具创建和管理 VDO 卷作为原生 LVM 逻辑卷。

VDO 提供内联块级 deduplication、压缩和精简置备功能。

如需更多信息，请参阅 [RHEL 中的编辑和压缩逻辑卷](#)。

(BZ#1598199)

### SCSI 堆栈现在可以更好地用于高性能适配器

SCSI 堆栈的性能有所提高。因此，在 RHEL 上，下一代高性能主机总线适配器(HBA)能够带来更高的 IOPS（每秒 I/O）。

(BZ#1761928)

### megaraid\_sas 驱动已更新至最新版本

**megaraid\_sas** 驱动已更新为版本 07.713.01.00-rc1。这个版本提供了几个与改进性能、支持 MegaRAID 适配器的稳定性以及更丰富的功能集相关的程序错误修复和增强。

(BZ#1791041)

### stratis 现在根据错误列出池名称

当您试图在现有 Stratis 池已经使用的块设备中创建 Stratis 池时，**stratis** 程序现在会报告现有池的名称。在以前的版本中，实用程序只列出池的 UUID 标签。

(BZ#1734496)

### FPIN ELS 框架通知支持

**lppc** 光纤通道(FC)驱动程序现在支持关于链路完整性的光纤性能影响通知(FPIN)，这有助于识别链路级问题，允许交换机选择更可靠的路径。

(BZ#1796565)

### 用于 LVM on-disk 元数据故障排除的新命令

**pvck** 工具可在 **lvm2** 软件包中使用，它现在提供低级命令来调试或者救援物理卷中的 LVM on-disk 元数据

- 要提取元数据，请使用 **pvck --dump** 命令。
- 要修复元数据，请使用 **pvck --repair** 命令。

如需更多信息，请参阅 **pvck(8)** man page。

(BZ#1541165)

## LVM RAID 支持 DM 完整性，以防止因为设备中的数据损坏而丢失数据

现在，可以将设备映射器(DM)完整性添加到 LVM RAID 配置中，以防止数据丢失。完整性层探测到设备中的数据崩溃，并警告 RAID 层以在 LVM RAID 中修复损坏的数据。

当 RAID 防止设备失败造成数据丢失时，在 LVM RAID 阵列中添加完整性可防止因为设备中数据损坏而丢失数据。您可在创建新 LVM RAID 时添加完整性层，或者您可以将其添加到已存在的 LVM RAID 阵列中。

(JIRA:RHELPLAN-39320)

## AWS、Azure 和 Aliyun 公有云上支持弹性存储(GFS2)

随着在三大公有云平台（Amazon(AWS)、Microsoft(Azure)和 Alibaba(Aliyun)）上支持共享块设备的引入，弹性存储(GFS2)现在在这些平台上得到了支持。因此，现在 GFS2 是一个真正的混合云集群文件系统，可选择在内部和公有云中使用的。有关在 Microsoft Azure 和 AWS 上配置共享存储的详情，请参考在[公共云平台上部署 Red Hat Enterprise Linux 8](#)。有关在 Alibaba Cloud 中配置共享存储的详情，请参考在[Alibaba Cloud 上为 Red Hat High Availability Cluster 配置共享存储](#)。

(BZ#1900019)

## 用户空间现在支持最新的 `nfsdclid` 守护进程

用户空间现在支持最新的 `nfsdclid` 守护进程，这是唯一的命名空间识别客户端跟踪方法。此增强可确保客户打开或锁定从容器化 `knfsd` 守护进程中的恢复，而不会造成任何数据崩溃。

(BZ#1817756)

## `nconnect` 现在支持多个并发连接

在这个改进中，您可以使用 `nconnect` 功能创建到 NFS 服务器的多个并发连接，从而允许不同的负载均衡功能。使用 `nconnect=X` NFS 挂载选择（其中 X 是要使用的并行连接数）启用 `nconnect` 功能。当前限制为 16。

(BZ#1683394, BZ#1761352)

## 现在支持用于客户端信息跟踪的 `nfsdclid` 守护进程

有了这个增强，`nfsdclid` 守护进程是跟踪稳定存储上每个客户端信息的默认方法。因此，容器中运行的 NFS v4 允许客户端在服务器重启后回收打开或锁定。

(BZ#1817752)

## 5.1.10. 高可用性和集群

### `pacemaker` rebase 到版本 2.0.4

Pacemaker 集群资源管理器已升级到上游版本 2.0.4，它提供了大量的程序错误修复。

(BZ#1828488)

### 新的 `priority-fencing-delay` 集群属性

Pacemaker 现在支持新的 `priority-fencing-delay` 集群属性，它允许您配置一个双节点集群，以便在脑裂情况下，运行最少资源的节点是被隔离的节点。

`priority-fencing-delay` 属性可以设置为持续时间。这个属性的默认值为 0（禁用）。如果将此属性设置为非零值，并且 `priority` meta-attribute 至少是为一个资源配置的，那么在脑裂情形下，在其上运行的所有资源的具有最高组合优先级的节点将更有可能存活。

例如：如果您设置 `pcs resource defaults priority=1` 和 `pcs property set priority-fencing-delay=15s`，且没有设置其他优先级，那么运行最多资源的节点将更可能丢失，因为其他节点将在启动保护前等待 15 秒。如果特定资源比其他资源更重要，您可以赋予它更高的优先权。

如果为该克隆配置了优先级，运行可升级的克隆 master 角色的节点会得到额外的 1 点。

使用 `priority-fencing-delay` 设置的任何延迟都会添加到 `pcmk_delay_base` 和 `pcmk_delay_max` 隔离设备属性中的任何延迟。当两个节点具有相等的优先级，或者不是由于节点丢失的原因（例如，为资源监控器操作设置了 `on-fail=fencing`）需要对两个节点进行隔离时，这种行为允许一些延迟。如果同时使用，建议您将 `priority-fencing-delay` 属性设置为显著大于 `pcmk_delay_base` 和 `pcmk_delay_max` 之间最大延迟的值，以确保首选优先节点（确保优先节点是完全安全的）。

(BZ#1784601)

## 管理多组资源和操作默认配置的新命令

现在可以创建、列出、更改和删除多个资源组和操作默认值。当您创建一组默认值时，您可以指定一个包含 `esource` 和 `op` 表达式的规则。例如，这允许您为特定类型的所有资源配置默认值。列出现有默认值的命令现在在输出中包含多个默认值集。

- `pcs resource [op] defaults set create` 命令生成一个新的默认值集合。当使用这个命令指定规则时，只允许使用 `resource` 和 `op` 表达式，包括 `and`、`or` 和括号。
- `pcs resource [op] defaults set delete | remove` 命令删除默认值。
- `pcs resource [op] defaults set update` 命令更改默认值。

(BZ#1817547)

## 支持标记集群资源

现在可以使用 `pcs tag` 命令在 Pacemaker 集群中标记集群资源。这个功能允许您使用单个命令管理一组指定的资源。您还可以使用 `pcs tag` 命令删除或修改资源标签，并显示标签配置。

`pcs resource enable`、`pcs resource disable`、`pcs resource manage` 和 `pcs resource unmanage` 命令接受 tag ID 作为参数。

(BZ#1684676)

## pacemaker 现在通过降级一个被提升的资源而不是完全停止它来支持恢复

现在，可以在 Pacemaker 集群中配置可升级的资源，这样在对资源执行升级或监控操作失败，或在其中运行资源的分区丢失仲裁时，该资源将被降级，但不会完全停止。

如果您希望资源在未升级模式中仍然可用，则这个功能很有用。例如，如果主数据库的分区丢失仲裁，您可能希望数据库资源失去 **Master** 角色，但在只读模式下保持活动状态，这样尽管失去了仲裁，仅需要读取的应用程序也能够继续运行。当成功降级足以恢复，且比完全重启快得多时，此功能也很有用。

支持此功能：

- `on-fail` 操作 meta-attribute 现在接受与 `promote` 操作一起使用的 `demote` 值，例如：

```
pcs resource op add my-rsc promote on-fail="demote"
```

- `on-fail` 操作 meta-attribute 现在接受与 `monitor` 操作一起使用的 `demote` 值，这个操作的 `interval` 设置为一个非零值，`role` 设置为 **Master**。例如：

```
pcs resource op add my-rsc monitor interval="10s" on-fail="demote" role="Master"
```



- **no-quorum-policy** 集群属性现在接受 **demote** 值。当设置时，如果集群分区缺少仲裁，任何提升的资源都会降级但会继续运行，所有其他资源将会停止。

为操作指定 **demote** meta-attribute 不会影响如何决定资源推广。如果受影响的节点仍然具有最高的升级分数，则会选择再次提升。

(BZ#1837747, [BZ#1843079](#))

### 新的 **SBD\_SYNC\_RESOURCE\_STARTUP** SBD 配置参数，以改进与 Pacemaker 的同步

为了更好地控制 SBD 和 Pacemaker 之间的同步，`/etc/sysconfig/sbd` 文件现在支持 **SBD\_SYNC\_RESOURCE\_STARTUP** 参数。当安装了 RHEL 8.3 或更高版本的 Pacemaker 和 SBD 软件包，并使用 **SBD\_SYNC\_RESOURCE\_STARTUP=true** 配置了 SBD 时，SBD 会联系 Pacemaker 守护进程以了解有关守护进程状态的信息。

在这个配置中，Pacemaker 守护进程会等待指定 SBD 联系后（在子守护进程启动前，且最终退出前）。因此，如果 SBD 无法与它进行活跃通讯，Pacemaker 将不会运行资源，而 Pacemaker 在它向 SBD 报告安全关闭前不会退出。这可以防止一个不太可能出现的情况：当 SBD 在 Pacemaker 最后断开连接前没有运行任何资源时，安全关闭期间可能会出现的问题，这会导致不必要的重启。使用一个定义的握手来检测安全关闭也可以在维护模式下工作。以前在没有运行的资源的情况下检测安全关闭的方法需要在维护模式中禁用，因为运行的资源不会在关机时受到影响。

另外，启用此功能可避免当 SBD 和 Pacemaker 可以成功启动但 SBD 无法联系 pacemaker 时，避免了在集群中出现分割崩溃的风险。这可能会发生，例如因为 SELinux 策略。在这种情况下，Pacemaker 假设 SBD 在不工作时可以正常工作。启用这个新功能后，Pacemaker 在 SBD 联系之前不会完成启动。这个新功能的另一个优点是，当启用 SBD 时，它会重复使用 heartbeat 联络 Pacemaker，如果 Pacemaker 停止响应，它可以随时阻塞节点。



#### 注意

如果编辑了 `/etc/sysconfig/sbd` 文件或者通过 PCS 配置 SBD，那么 RPM 升级将不会拉取新的 **SBD\_SYNC\_RESOURCE\_STARTUP** 参数。在这些情况下，要实现这个功能，您必须手动在 `/etc/sysconfig/sbd.rpmnew` 文件中添加它，或者按照 **sbd** (8) 手册页中的 **Configuration via environment** 部分中描述的步骤进行添加。

(BZ#1718324, [BZ#1743726](#))

## 5.1.11. 动态编程语言、网页和数据库服务器

### 新模块流：**ruby:2.7**

RHEL 8.3 在新的 **ruby:2.7** 模块流中引入了 Ruby 2.7.1。这个版本对 RHEL 8.1 提供的 Ruby 2.6 版本提供了很多性能改进、程序错误和安全性修复以及新的功能。

主要改进包括：

- 增加了新的 Compaction Garbage Collector (GC)。这个 GC 可以对碎片化内存进行处理。
- Ruby yet Another Compiler-Compiler (Racc) 现在提供了一个命令行界面用于 one-token Look-Ahead Left-to-Right - LALR(1) - parser generator。
- 交互式 Ruby Shell (**irb**) (捆绑的 Read-Eval-Print Loop (REPL) 环境) 现在支持多行编辑。
- 模式匹配是作为实验功能引进的，经常在功能编程语言中使用。

- 已引进了作为默认块参数的编号参数作为一个实验性功能。

改进的性能：

- 光纤缓存策略已被修改来加快光纤的创建速度。
- 提高了 **CGI.escapeHTML** 方法的性能。
- **Monitor** 类和 **MonitorMixin** 模块的性能有所改进。

另外，关键字参数和位置参数的自动转换已被弃用。在 Ruby 3.0 中， positional 参数和 keyword 参数将被分开。如需更多信息，请参阅 [上游文档](#)。

要绕过针对实验功能的警告，请使用 **-W:no-experimental** 命令行选项。要禁用弃用警告，请使用 **-W:no-deprecated** 命令行选项，或者在您的代码中添加 **Warning[:deprecated] = false**。

要安装 **ruby:2.7** 模块流，请使用：

```
# yum module install ruby:2.7
```

如果要从 **ruby:2.6** 流升级，请参阅[切换到更新的流](#)。

(BZ#1817135)

### 新模块流：nodejs:14

现在提供了一个新的模块流 **nodejs:14**。**Node.js 14** 包含在 RHEL 8.3 中，与 RHEL 8.1 中的 **Node.js 12** 相比，提供了大量新功能、错误和安全修复。

主要变更包括：

- V8 引擎已升级至 8.3。
- 实施了一个新的实验性 WebAssembly 系统接口（WASI）。
- 引入了一个新的实验性 Async Local Storage API。
- 现在，诊断报告的功能是稳定的。
- streams API 已强化。
- 已删除实验性模块警告。

随着 [RHEA-2020:5101](#) 公告的发布，RHEL 8 提供了 **Node.js 14.15.0**，它是最新的长期支持(LTS)版本，具有更高的稳定性。

要安装 **nodejs:14** 模块流，使用：

```
# yum module install nodejs:14
```

如果要从 **nodejs:12** 流升级，请参阅[切换到更新的流](#)。

(BZ#1815402, [BZ#1891809](#))

### git rebase 到版本 2.27

**git** 软件包已升级到上游版本 2.27。之前发布的 2.18 版本的显著变化包括：

- **git checkout** 命令已经被分成两个独立命令：
  - **git switch** 用于管理分支
  - **git restore** 用于管理目录树中的变化
- **git rebase** 命令的行为现在默认基于 **merge** 工作流，而不是之前的 **patch+apply** 工作流。要保留之前的行为，把 **rebase.backend** 配置变量设置为 **apply**。
- **git difftool** 命令现在可以在程序库之外使用。
- 引进了四个新配置变量 **{author,committer}.{name,email}**，以便在更具体的情况下覆盖 **user.{name,email}**。
- 添加了几个新选项可让用户配置 SSL 进行与代理沟通。
- 以非 UTF-8 字符编码处理日志消息的提交在 **git fast-export** 和 **git fast-import** 工具中得到了改善。
- **lfs** 扩展已添加为一个新的 **git-lfs** 软件包。Git 大文件存储(LFS)在 **Git** 中使用文本指针替代大型文件，并将文件内容存储在远程服务器上。

([BZ#1825114](#), [BZ#1783391](#))

## Python的更改

RHEL 8.3 对 **python38:3.8** 模块流包括以下更改：

- **Python** 解释器已更新至 3.8.3 版本,它提供一些程序错误修复。
- **python38-pip** 软件包已更新至版本193.1,现在 **pip** 支持安装许多 **linux2014** wheels。

由 **python3** 软件包提供的 **Python 3.6** 解释器性能显著提高。

**ubi8/python-27**,**ubi8/python-36** 和 **ubi8/python-38** 容器镜像现在支持从自定义软件包索引或 PyPI 镜像（如果客户提供了）安装 **pipenv** 工具。在以前的版本中，**pipenv** 只能从上游 PyPI 存储库下载，如果上游存储库不可用，安装会失败。

([BZ#1847416](#),[BZ#1724996](#),[BZ#1827623](#), [BZ#1841001](#))

## 新模块流：php:7.4

RHEL 8.3 引入了 **PHP 7.4**，它比版本 7.3 提供了很多程序错误修复和增强。

此发行版本引入了一个新的实验性扩展 - Foreign Function Interface (FFI)，它可让您调用原生功能、访问原生变量以及创建和访问 C 库中定义的数据结构。FFI 扩展包括在 **php-ffi** 软件包中。

删除了以下扩展：

- 从 **php-xml** 软件包中删除 **wddx** 扩展
- 从 **php-recode** 软件包中删除 **recode** 扩展。

要安装 **php:7.4** 模块流，请使用：

```
# yum module install php:7.4
```

如果要从 **php:7.3** 流升级，请参阅[切换到更新的流](#)。

有关 RHEL 8 中 PHP 使用的详情，请参阅[使用 PHP 脚本语言](#)。

([BZ#1797661](#))

### 新模块流：nginx:1.18

**nginx 1.18** 网页和代理服务器，与版本 1.16 相比，提供多个程序错误修复、安全修复、新功能以及改进。主要变更包括：

- 实现了对 HTTP 请求率和连接限制的增强。例如：**limit\_rate** 和 **limit\_rate\_after** 指令现在支持变量,其中包括新的 **\$limit\_req\_status** 和 **\$limit\_conn\_status** 变量。另外，为 **limit\_conn\_dry\_run** 和 **limit\_req\_dry\_run** 指令增加了 dry-run 模式。
- 添加了一个新的 **auth\_delay** 指令，它可启用对未授权请求的处理延迟。
- 以下指令现在支持变量：**grpc\_pass**、**proxy\_upload\_rate** 和 **proxy\_download\_rate**。
- 添加了额外的 PROXY 协议变量，即 **\$proxy\_protocol\_server\_addr** 和 **\$proxy\_protocol\_server\_port**。

要安装 **nginx:1.18** 流，请使用：

```
# yum module install nginx:1.18
```

如果要从 **nginx:1.16** 流升级，请参阅[切换到更新的流](#)。

([BZ#1826632](#))

### 新模块流：perl:5.30

RHEL 8.3 引进了 **Perl 5.30**，它比之前发布的 **Perl 5.26** 提供了很多 bug 修复和增强。新版本还会弃用或删除某些语言功能。显著影响变化包括：

- **Math::BigInt::CalcEmu**、**arybase** 和 **B::Debug** 模块已被删除
- 现在使用一个 **close-on-exec** 标记打开文件描述符
- 不再允许打开和文件和目录句柄相同的符号
- 现在，subroutine 属性必须在 subroutine 签名前进行。
- **:locked** 和 **:uniq** 属性已删除
- 不再允许没有使用逗号分隔的变量列表
- 不再允许使用裸 **<<** here-document 操作符
- 在正则表达式中使用未转义的左括号 (**{**) 不再允许
- **AUTOLOAD()** 子程序无法再继承到非方法函数
- **sort** 不再允许指定 **sort** 算法
- **B::OP::terse()** 子函数已被 **B::Concise::b\_terse()** 子函数替代
- **File::Glob::glob()** 功能已被 **File::Glob::bsd\_glob()** 功能替代
- **dump()** 功能现在必须通过 **CORE::dump()** 调用

- yada-yada operator (...) 现在是一个声明，它不能作为一个表达式
- 为 \$[ 变量分配一个非零值，现在返回一个致命错误
- 不再允许 \$\* 和 \$# 变量
- 不再允许在 false 条件分支中使用 my() 函数来定义变量
- 在 :utf8 handles 上使用函数 sysread() 和 syswrite() 现在返回一个致命的错误
- pack() 函数不再返回不正确的 UTF-8 格式
- 不再允许值大于 IV\_MAX 的 Unicode 代码点
- Unicode 12.1 现在被支持

要从以前的 perl 模块流升级，请参阅 [切换到更新的流](#)。

Perl 5.30 还可作为 s2i-enabled ubi8/perl-530 容器镜像提供。

([BZ#1713592](#), [BZ#1732828](#))

#### 新模块流：perl-libwww-perl:6.34

RHEL 8.3 引进了新的 perl-libwww-perl:6.34 模块流，它为 RHEL 8 中的所有 Perl 版本提供 perl-libwww-perl 软件包。从 RHEL 8.0 开始，非 modular perl-libwww-perl 软件包（它不能与 5.26 之间的其它 Perl 流一起使用）已被新的默认 perl-libwww-perl:6.34 stream 弃用。

([BZ#1781177](#))

#### 新模块流：perl-IO-Socket-SSL:2.066

现在提供了一个新的 perl-IO-Socket-SSL:2.066 模块流。这个模块提供 perl-IO-Socket-SSL 和 perl-Net-SSLeay 软件包，并与 RHEL 8 中的所有 Perl 流兼容。

([BZ#1824222](#))

#### squid:4 模块流恢复到版本 4.11

Squid 代理服务器由 squid:4 模块流提供，已从版本 4.4 升级到 4.11。此发行版本提供多个程序错误和安全修复以及各种增强，如新的配置选项。

([BZ#1829467](#))

#### httpd:2.4 模块流中的更改

RHEL 8.3 对 Apache HTTP 服务器包括以下显著更改，这些更改可通过 httpd:2.4 模块流提供：

- mod\_http2 模块被 rebase 到版本 1.15.7
- H2Upgrade 和 H2Push 指令的配置已改变
- 新的 H2Padding 配置指令，用于控制 HTTP/2 有效负载数据帧的 padding
- 修复多个程序错误。

([BZ#1814236](#))

支持从 httpd 中的 CustomLog 指令登录到 journald

现在你可以使用 **CustomLog** 指令的新选项将 Apache HTTP 服务器的 **journald** 输出到 **journald**。

支持语法如下：

```
CustomLog journald:priority format|nickname
```

其中 *priority* 是 **LogLevel** 指令中使用的任何优先级字符串，最高为 **debug**。

例如，要使用 **combined** 日志格式在 **journald** 中记录日志，请使用：

```
CustomLog journald:info combined
```

请注意,当使用这个选项时，服务器性能可能会低于使用在一个平面文件中直接记录日志。

([BZ#1209162](#))

## 5.1.12. 编译器和开发工具

### .NET 5 现在包括在 RHEL 中

.NET 5 在 Red Hat Enterprise Linux 7、Red Hat Enterprise Linux 8 和 OpenShift Container Platform 中提供。.NET 5 包括新的语言版本：C# 9 和 F#5.0。基本程序库的性能有显著提高。GC 和 JIT。.NET 5 有单一文件应用程序，用户可以使用一个可执行文件来发布 .NET 应用程序，所有的依赖程序都包括在这个文件中。Red Hat 容器 registry 提供了 .NET 5 的 UBI8 镜像，它们可用于 OpenShift。

要使用 .NET 5，安装 **dotnet-sdk-5.0** 软件包：

```
$ sudo dnf install -y dotnet-sdk-5.0
```

如需更多信息，请参阅 [.NET 5 文档](#)。

([BZ#1944677](#))

### 新的 GCC 工具集 10

GCC 工具集 10 是提供开发工具最新版本的编译器工具组。它在 **AppStream** 存储库中以软件集合的形式作为应用程序流提供。

GCC 编译器已更新至版本 10.2.1，它在上游 GCC 中提供了很多程序错误修复和增强。

GCC 工具集 10 提供以下工具和版本：

工具	版本
GCC	10.2.1
GDB	9.2
Valgrind	3.16.0
SystemTap	4.3
Dyninst	10.1.0

工具	版本
binutils	2.35
elfutils	0.180
dwz	0.12
make	4.2.1
strace	5.7
ltrace	0.7.91
annobin	9.29

要安装 GCC Toolset 10，请以根用户身份运行以下命令：

```
# yum install gcc-toolset-10
```

要从 GCC Toolset 10 运行工具：

```
$ scl enable gcc-toolset-10 tool
```

要运行一个 shell 会话，其中的 GCC Toolset 10 中的工具版本会覆盖这些工具的系统版本：

```
$ scl enable gcc-toolset-10 bash
```

如需更多信息，请参阅 [使用 GCC 工具集](#)。

GCC Toolset 10 组件在两个容器镜像中可用：

- **rhel8/gcc-toolset-10-toolchain**，包括 GCC 编译器、GDB 调试器和 **make** 自动化工具。
- **rhel8/gcc-toolset-10-perftools**，其中包括性能监控工具，如 SystemTap 和 Valgrind。  
要拉取容器镜像，以 root 身份运行以下命令：

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

请注意，现在只支持 GCC Toolset 10 容器镜像。之前 GCC Toolset 版本的容器镜像已弃用。

有关容器镜像的详情，请参阅 [使用 GCC 工具集容器镜像](#)。

(BZ#1842656)

## Rust Toolset 被 rebase 到版本 1.45.2

Rust Toolset 已更新至 1.452 版本。主要变更包括：

- 用于查看依赖关系的子命令的 **cargo tree** 现在包含在 **cargo** 中。

- 现在从浮点值转换到整数时会使用一个范围保护。在以前的版本中，当转换浮点值时，如果被简化的浮点值超出了目标整数类型的范围时，编译器会认为是未定义（undefined）非限定浮动点值也会导致未定义的行为。在这个改进中，有限值被声明为整数的最小值或最大范围。正无限值和负无限值会分别默认为最大整数值和最小整数值，Not-a-Number(NaN) 值为零。
- 现在，表达式、模式和声明等类似于函数的程序宏被扩展并稳定。

有关使用方法的详细信息，[请参阅使用 Rust Toolset](#)。

(BZ#1820593)

### LLVM Toolset rebase 到版本 10.0.1

LLVM Toolset 升级至版本 10.0.1。在这个版本中，**clang-libs** 软件包不再包含各个组件库。因此，无法再连接针对它们的应用程序。要根据 **clang** 库链接应用程序，使用 **libclang-cpp.so** 软件包。

如需更多信息，[请参阅使用 LLVM Toolset](#)。

(BZ#1820587)

### Go Toolset rebase 到版本 1.14.7

Go Toolset 已经升级至 1.14.7 版，新的变更包括：

- Go 模块系统现已获得全面支持。
- 不再支持 SSL 版本 3.0(SSLv3)。Delve debugger 的主要改进包括：
- 新命令 **examinemem**（或 **x**）检查原始内存
- 新命令 **display** 在程序每次停止时打印一个表达式的值
- 为调试程序提供 Teletypewriter(TTY)的新 **--tty** 标志
- Arm64 的新 **coredump** 支持
- 打印 goroutine 标签的新功能
- 发布 Debug Adapter Protocol(DAP)服务器
- 改进了 **dlv trace** 和 **trace REPL**（read-eval-print-loop）命令的输出

有关 Go Toolset 的详情，[请参考使用 Go Toolset](#)。

有关 Delve 的更多信息，[请参见上游 Delve 文档](#)。

(BZ#1820596)

### SystemTap rebase 到版本 4.3

SystemTap 工具已更新至版本 4.3，提供多个程序错误修复和增强。主要变更包括：

- 用户空间探测可以通过 **readelf -n** 的十六进制 **buildid** 作为目标。这种路径名称的替代方案允许在任何名称下探测匹配的二进制文件，从而允许单个脚本以一系列不同版本为目标。这个功能可以和 elfutils **debuginfod** 服务器一起正常工作。
- 脚本函数可以使用探测 **\$context** 变量访问探测位置中的变量，这使得 SystemTap 脚本能够使用通用逻辑与各种探测一起工作。



- 已经进行了 **stapbpf** 程序改进，包括 try-catch 语句和错误探测，以便在 BPF 后端上运行的脚本中启用适当的容错。

有关显著变化的详情，请在更新前阅读 [上游发行注记](#)。

(BZ#1804319)

## Valgrind 被 rebase 到版本 3.16.0

Valgrind 可执行文件代码分析工具已更新至版本 3.16.0，与之前的版本相比，它提供了一些 bug 修复和增强：

- 现在，如果您的程序在 Valgrind 下运行（通过 **vgdb**，通过一个 **gdb** 连接到 Valgrind gdbserver，或通过程序客户端请求），可以动态地修改许多命令行参数的值。要获得可更改的选项列表，请运行 **valgrind --help-dyn-options** 命令。
- 对于 Cachegrind (**cg\_annotate**) 和 Callgrind (**callgrind\_annotate**) 工具，**--auto** 和 **--show-percs** 选项现在默认为 **yes**。
- Memcheck 工具在优化代码时生成较少的假错误。特别是 Memcheck 现在更好地处理编译器将 **A && B** 检查转换为 **B && A** 检查的情况，其中 **B** 可以是未定义，**A** 为 false。memcheck 也能更好地处理对部分定义值的整数相等性检查和非相等性检查。
- 试验性的 Stack and Global Array Checking 工具 (**exp-sgcheck**) 已被删除。它的功能可以由 GCC 的 AddressSanitizer(ASAN)工具替代，这需要您使用 **-fsanitize=address** 选项重建代码。

(BZ#1804324)

## elfutils rebase 到版本 0.180

elfutils 软件包更新至 0.180 版本，提供多个程序错误修复和增强。主要变更包括：

- 更好地支持 GCC LTO 构建的代码调试信息（链接时间优化）。**eu-readelf** 和 **libdw** 程序现在可以读取和处理 **.gnu.debuglto\_** 部分，并正确地解析跨 CU（组合单元）定义的功能的文件名。
- **eu-nm** 程序现在明确将弱对象定义为 **V**，常见符号为 **C**。
- **debuginfod** 服务器现在可以对 **.deb** 归档进行索引，并有通用扩展以添加其它软件包归档格式（使用 **-Z EXT[=CMD]** 选项）。例如，**-Z '.tar.zst=zstdcat'** 表示以 **.tar.zst** 扩展结尾的归档应该使用 **zstdcat** 程序解包。
- **debuginfo-client** 工具有几个新的帮助程序功能，如 **debuginfod\_set\_user\_data**、**debuginfod\_get\_user\_data**、**debuginfod\_get\_url** 和 **debuginfod\_add\_http\_header**。它现在还支持 **file:// URL**。

(BZ#1804321)

## GDB 现在支持在 IBM z15 上的进程记录和重新进行

在这个版本中，GNU Debugger (GDB) 支持进程记录，并使用 IBM z15 处理器的大部分新指令（以前称为 arch13）进行重播。请注意，当前不支持以下指令：SORTL（排序列表）、DFLTCC（删除转换调用）、KDSA（计算数字签名身份验证）。

(BZ#1659535)

## 在 papi 中更新了 Marvell ThunderX2 性能监控事件

在这个版本中，很多特定于 ThunderX2 的性能事件（包括非核事件）已被更新。因此，开发人员可以更好地调查 Marvell ThunderX2 系统的系统性能。

(BZ#1726070)

### glibc math 库现在为 IBM Z 进行了优化

在这个版本中，**libm** math 功能进行了优化，可以提高 IBM Z 机器的性能。主要变更包括：

- 改进了循环模式处理，以避免多余的浮点控制集和提取
- 利用 z196 整数和浮点之间的转换

(BZ#1780204)

### 现在提供了额外的特定于 libffi 的临时目录

之前在强化型系统中，系统范围内的临时目录可能没有适合 **libffi** 库的权限。

在这个版本中，系统管理员可以设置 **LIBFFI\_TMPDIR** 环境变量指向 **libffi** 特定的临时目录，并具有 **write** 和 **exec** mount 或 **selinux** 权限。

(BZ#1723951)

### 提高了 strstr() 和 strcasestr() 的性能

在这个版本中，在几个支持的构架中，**strstr()** 和 **strcasestr()** 函数的性能已改进。现在，所有使用字符串和内存操作程序的应用程序性能可以提高用户的性能。

(BZ#1821531)

### glibc 现在可以正确加载被截断的区域归档

如果之前截断了系统本地的归档，在升级过程中出现断电或磁盘失败，进程可能会在加载归档时意外终止。这个改进为加载语言归档增加了一致性检查。现在，进程可以检测到归档中继并回退到非构架安装的区域或默认的 POSIX 区域。

(BZ#1784525)

### GDB 现在支持 debuginfod

有了这个增强，GNU Debugger(GDB)现在可以使用 **elfutils debuginfod** 客户端库按需从集中式服务器下载调试信息软件包。

(BZ#1838777)

### pcp rebase 到版本 5.1.1-3

**pcp** 软件包已升级至版本 5.1.1-3。主要变更包括：

- 更新服务单元，改进了所有 PCP 服务的 **systemd** 集成和可靠性。改进了归档日志轮转并更及时地进行压缩。**pmproxy** 协议中的归档发现程序错误被修复。
- 改进了 **pcp-atop**、**pcp-dstat**、**pmrep** 和相关的监控工具，以及 **pmrep** 和导出工具中的指标标签。
- 改进了 **bpftrace**、**OpenMetrics**、**MMV**、Linux 内核代理和其他集合代理。**Open vSwitch** 和 **RabbitMQ** 服务器的新指标收集器。
- 新的主机发现 **pmfind systemd** 服务替换独立 **pmmgr** 守护进程。

(BZ#1792971)

## grafana rebase 到版本 6.7.3

**grafana** 软件包已更新至 6.7.3 版本。主要变更包括：

- 通用 **OAuth** 角色映射支持
- 新的日志面板
- 在表面板中显示多行文本
- 新的货币单位和能源单位

([BZ#1807323](#))

## grafana-pcp rebase 到版本 2.0.2

**grafana-pcp** 软件包已更新至版本 2.0.2。主要变更包括：

- 支持在 **flamegraph** 中显示多维 eBPF 映射。
- 删除查询编辑器中的自动完成缓存，以便 PCP 指标可以动态显示。

([BZ#1807099](#))

## 新的 rhel8/pcp 容器镜像

**rhel8/pcp** 容器镜像现在包括在 Red Hat Container Registry 中。镜像包含 Performance Co-Pilot(PCP) 工具包，其中包括预安装的 **pcp-zeroconf** 软件包和 **OpenMetrics** PMDA。

([BZ#1497296](#))

## 新的 rhel8/grafana 容器镜像

**rhel8/grafana** 容器镜像现在包括在 Red Hat Container Registry 中。Grafana 是一个开源实用程序，它带有 metrics dashboard,以及 **Graphite**、**Elasticsearch**、**OpenTSDB**、**Prometheus**、**InfluxDB** 和 **PCP** 监控工具的图形编辑器。

([BZ#1823834](#))

## 5.1.13. 身份管理

### IdM 备份工具现在检查所需的副本角色

**ipa-backup** 工具现在检查 IdM 集群中使用的所有服务，如证书颁发机构(CA)、域名系统(DNS)和密钥恢复代理(KRA)是否安装在您要运行备份的副本上。如果副本没有安装所有的服务，**ipa-backup** 程序会以警告方式退出，因为在该主机上进行的备份不足以完全恢复集群。

例如，如果您的 IdM 部署使用集成证书认证机构 (CA)，非副本中运行的备份将无法捕获 CA 数据。红帽建议验证执行 **ipa-backup** 的副本是否在集群安装中使用了所有 IdM 服务。

如需更多信息，请参阅[准备使用 IdM 备份数据丢失](#)。

([BZ#1810154](#))

### 新的密码过期通知工具

由 **ipa-client-epn** 软件包提供的过期密码通知(EPN)是一个独立的工具，您可以用来构建密码即将过期的身份管理(IdM)用户的列表。

IdM 管理员可以使用 EPN 进行以下操作：

- 以 JSON 格式显示受影响用户列表，该列表在运行时计算
- 计算在给定日期或日期范围内发送多少封电子邮件
- 向用户发送密码过期电子邮件通知

红帽建议每天从 IdM 客户端或使用 `ipa-epn.timer systemd` 计时器启动一次 EPN。

(BZ#913799)

## JSS 现在提供 FIPS 兼容 SSLContext

之前，Tomcat 使用来自 Java 加密架构(JCA)SSLContext 类的 SSLContext 指令。默认的 SunJSSE 实现不符合联邦信息处理标准(FIPS)，因此 PKI 现在通过 JSS 提供符合 FIPS 的实现。

(BZ#1821851)

## 现在可以使用检查您的公钥基础架构的整体健康状况

有了这个更新，公钥基础架构(PKI) Healthcheck 工具向 RHEL 8.1 中引入的身份管理(IdM) Healthcheck 工具报告 PKI 子系统的健康状况。执行 IdM Healthcheck 会调用 PKI Healthcheck，它会收集并返回 PKI 子系统的健康状况报告。

所有部署的 RHEL IdM 服务器或副本都提供了 `pki-healthcheck` 工具。`pki-healthcheck` 提供的所有检查也集成到 `ipa-healthcheck` 工具中。`ipa-healthcheck` 可以与 `idm:DL1` 模块流安装分开安装。

请注意，`pki-healthcheck` 也可以在独立 Red Hat 证书系统(RHCS)基础架构中正常工作。

(BZ#1770322)

## 支持 RSA PSS

在这个版本中，PKI 支持 RSA PSS（安全签名方案）签名算法。

要启用此功能，在 `pkispawn` 脚本文件中为给定子系统设置以下行：

```
pki_use_pss_rsa_signing_algorithm=True
```

因此，此子系统的所有现有的默认签名算法（在其 `CS.cfg` 配置文件中指定）将使用相应的 PSS 版本。例如，`SHA256withRSA` 变为 `SHA256withRSA/PSS`

(BZ#1824948)

## 在服务启动时，目录服务器将私钥和证书导出到私有命名空间中

目录服务器使用 OpenLDAP 库进行外部连接，比如复制协议。由于这些库无法直接访问网络安全服务(NSS)数据库，目录服务器会从带有 TLS 加密支持的实例上的 NSS 数据库提取私钥和证书，使 OpenLDAP 库能够建立加密的连接。在以前的版本中，目录服务器将私钥和证书提取到 `cn=config` 条目（默认为 `/etc/dirsrv/slapd-<instance_name>`）中 `thenslapd-certdir` 参数中设置的目录。因此，Directory 服务器将 `Server-Cert-Key.pem` 和 `Server-Cert.pem` 保存在这个目录中。在这个改进中，Directory 服务器提取私钥和证书给 `systemd` 挂载到 `/tmp/` 目录中的专用命名空间。因此，增加了安全性。

(BZ#1638875)

## 如果达到磁盘监控阈值，则目录服务器现在可以将实例切换到只读模式

这个版本在 `cn=config` 条目中添加 `nsslapd-disk-monitoring-readonly-on-threshold` 参数。如果您启

用这个设置，在启用了磁盘监控且可用磁盘空间低于您在 `nsslapd-disk-monitoring-threshold` 中配置的值时，Directory 服务器会将所有数据库切换成只读。如果将 `nsslapd-disk-monitoring-readonly-on-threshold` 设置为 `on`，则数据库无法修改，直到 Directory 服务器成功关闭该实例。这可以防止数据崩溃。

(BZ#1728943)

### samba rebase 到版本 4.12.3

`samba` 软件包升级至上游版本 4.12.3，比之前的版本提供了很多程序错误修复和增强：

- 内置的加密功能已被 GnuTLS 功能替代。这提高了服务器消息块版本 3(SMB3)性能，复制速度显著提高。
- 现在，最小运行时版本是 Python 3.5。
- 删除了 `write cache size` 参数，因为以前的写入缓存概念可能会降低内存约束系统的性能。
- 删除了对使用带有 DES 加密类型的 Kerberos ticket 验证连接的支持。
- `vfs_netatalk` 虚拟文件系统(VFS)模块已被删除。
- `ldap ssl ads` 参数标记为已弃用,并将在以后的 Samba 版本中删除。有关如何加密 LDAP 流量和详情的详情请参考 [samba: removal of "ldap ssl ads" smb.conf option](#)。
- 默认情况下，RHEL 8.3 中的 Samba 不再支持过时的 RC4 密码套件。如果您在 AD 中作为域成员运行 Samba，仍然需要 Kerberos 验证的 RC4,请使用 `update-crypto-policies --set DEFAULT:AD-SUPPORT` 命令启用对 RC4 加密类型的支持。

当 `smbd`、`nmbd` 或者 `winbind` 服务启动时，Samba 会自动更新它的 `tdb` 数据库文件。在启动 Samba 前备份数据库文件。请注意，红帽不支持降级 `tdb` 数据库文件。

有关显著变化的详情，请在更新前阅读 [上游发行注记](#)。

(BZ#1817557)

### cockpit-session-recording rebase 到版本 4

`cockpit-session-recording` 模块更新到版本 4。此版本提供以下与上一个版本相比的显著变化：

- 更新了 `metainfo` 文件中的父 ID。
- 更新软件包清单。
- 修复了 `rpmmacro` 以解析 CentOS7 上正确的路径。
- 处理由 `byte-array` 编码的日志数据。
- 将代码从已弃用的 React 生命周期功能中移出。

(BZ#1826516)

### krb5 rebase 到版本 1.18.2

`krb5` 软件包已升级到上游版本 1.18.2。重要的修复和增强包括：

- 删除了 `single-DES` 和 `triple-DES` 加密类型。
- 第 9 章 PKINIT 已被删除，因为所有受支持的 Active Directory 版本都不需要它。

- NegoEx 机制插件现在被支持。
- Hostname canonicalization fallback 现在支持 (`dns_canonicalize_hostname = fallback`) 。

(BZ#1802334)

### IdM 现在支持新的 Ansible 管理模块

此更新引入了几个 **ansible-freeipa** 模块，用于使用 Ansible playbook 自动完成通用身份管理(IdM)任务：

- **config** 模块允许在 IdM 中设置全局配置参数。
- **dnsconfig** 模块允许修改全局 DNS 配置。
- **dnsforwardzone** 模块允许在 IdM 中添加和删除 DNS 转发程序。
- **dnsrecord** 允许管理 DNS 记录。与上游 **ipa\_dnsrecord** 不同，它允许在一次执行中进行多个记录管理，并支持更多记录类型。
- **dnszone** 模块允许在 DNS 服务器中配置区。
- **service** 允许确保存在服务或不存在服务。
- **vault** 模块可保证 vaults 和 vaults 成员的存在和不存在。

请注意，**ipagroup** 和 **ipahostgroup** 模块已扩展为分别包含用户和主机组成员资格管理器。组成员管理器是用户或组，它可以添加组群成员或从组中删除成员。如需更多信息，请参阅对应 `/usr/share/doc/ansible-freeipa/README-*` 文件的 **Variables** 部分。

(JIRA:RHELPLAN-49954)

### IdM 现在支持新的 Ansible 系统角色来管理证书

身份管理(IdM)支持新的 Ansible 系统角色来自动化证书管理任务。新角色包括以下优点：

- 该角色有助于自动运行和续订证书。
- 角色可以被配置为使 **ipa** 证书颁发机构签发您的证书。这样，您可以使用现有 IdM 基础架构来管理证书信任链。
- 角色允许您指定在签发证书之前和发出后要执行的命令，例如停止和启动服务。

(JIRA:RHELPLAN-50002)

### 身份管理现在支持 FIPS

有了这个增强，您现在可以使用联邦信息处理标准(FIPS)批准的加密类型以及身份管理(IdM)中的验证机制。请注意 IdM 和 Active Directory 间的跨林信任不兼容 FIPS。

需要 FIPS 但不需要 AD 信任的用户现在可以在 FIPS 模式中安装 IdM。

(JIRA:RHELPLAN-43531)

### idm:DL1 中的 OpenDNSSEC 更新到版本 2.1

**idm:DL1** 模块流的 OpenDNSSEC 组件已升级至 2.1 版本，这是当前上游支持版本。OpenDNSSEC 是一个开源项目，推动采用域名系统安全扩展(DNSSEC)，以进一步增强互联网安全性。OpenDNSSEC 2.1 提供了一些程序错误修正和增强。如需更多信息，请参阅上游发行注记：

<https://www.opendnssec.org/archive/releases/>

(JIRA:RHELPLAN-48838)

## IdM 现在支持弃用的 RC4 密码套件，并使用新的系统范围的加密子策略

这个更新引进了新的 **AD-SUPPORT** 加密子策略，其启用了身份管理(IdM)中的 Rivest Cipher 4(RC4)密码套件。

作为 IdM 活动目录(AD)跨林信任中的管理员，当 AD 没有配置为使用高级加密标准(AES)时，您可以激活新的 **AD-SUPPORT** 子策略。更具体地说，如果适用以下条件之一，红帽建议启用新的子策略：

- AD 中的用户或服务帐户具有 RC4 加密密钥且缺少 AES 加密密钥。
- 各个活跃目录域之间的信任链接具有 RC4 加密密钥，且缺少 AES 加密密钥。

除了 **DEFAULT** 加密策略外，要启用 **AD-SUPPORT** 子策略，请输入：

```
# update-crypto-policies --set DEFAULT:AD-SUPPORT
```

另外，若要在 AD 林中的 AD 域间升级信任以便支持强大的 AES 加密类型，请查看以下 Microsoft 文档 [AD DS: Security: Kerberos "Unsupported etype" error when accessing a resource in a trusted domain](#)。

(BZ#1851139)

## 根据新的 Microsoft LDAP 频道绑定和 LDAP 签名要求调整

有了最近的 Microsoft 更新，活动目录(AD)将标记不使用 LDAP 通道绑定和 LDAP 签名的默认的 Windows 设置的客户端。因此，使用系统安全服务守护进程(SSSD)直接或间接与 AD 集成的 RHEL 系统，在使用通用安全服务应用程序接口(GSSAPI)的简单认证和安全层(SASL)操作成功后，可能会在 AD 中触发错误事件 ID。

要防止这些通知，请将客户端应用程序配置为使用 Simple 和 Protected GSSAPI Negotiation 机制(GSS-SPNEGO)SASL 机制而不是 GSSAPI。要配置 SSSD,将 `ldap_sasl_mech` 选项设定为 **GSS-SPNEGO**。

另外，如果在 AD 端强制实施通道绑定，请通过以下方式配置任何使用带有 SSL/TLS 的 SASL 的系统：

1. 安装 RHEL 8.3 及更新版本提供的 **cyrus-sasl**、**openldap** 和 **krb5-libs** 软件包的最新版本。
2. 在 `/etc/openldap/ldap.conf` 文件中，通过将 **SASL\_CBINDING** 选项设置为 **tls-endpoint** 来指定正确的频道绑定类型。

如需更多信息，请参阅 [Microsoft 安全顾问 ADV190023 | LDAP Channel Binding 和 LDAP Signing 在 RHEL 和 AD 集成中的影响](#)。

(BZ#1873567)

## SSSD、adcli 和 realmd 现在支持弃用的 RC4 密码套件（带有新的系统范围加密子策略）

这个更新引进了新的 **AD-SUPPORT** 加密子策略，为以下工具启用了 Rivest Cipher 4(RC4)密码套件：

- 系统安全性服务守护进程(SSSD)
- **adcli**
- **realmd**

作为管理员，在以下情况下,当 Active Directory (AD) 没有配置为使用高级加密标准 (AES) 时，您可以激活新的 **AD-SUPPORT** 子策略：

- SSSD 用于直接连接到 AD 的 RHEL 系统。
- **adcli** 用于加入 AD 域或更新主机属性，例如主机密钥。
- **realmd** 用于连接 AD 域。

如果适用以下条件之一，红帽建议启用新的子策略：

- AD 中的用户或服务帐户具有 RC4 加密密钥且缺少 AES 加密密钥。
- 各个活跃目录域之间的信任链接具有 RC4 加密密钥，且缺少 AES 加密密钥。

除了 **DEFAULT** 加密策略外，要启用 **AD-SUPPORT** 子策略，请输入：

```
# update-crypto-policies --set DEFAULT:AD-SUPPORT
```

([BZ#1866695](#))

### authselect 有一个新的 minimal 配置集

**authselect** 程序有一个新的 **minimal** 配置集。您可以使用这个配置集直接从系统文件中提供本地用户和组群，而不必使用其它验证供应商。因此，可以安全地删除 **SSSD**、**winbind** 和 **fpntd**，并可在需要最小安装的系统中使用这个配置集保存磁盘和内存空间。

([BZ#1654018](#))

### SSSD 现在在轮转密码时更新 Samba 的 secret.tdb 文件

现在，在 RHEL 中提供了 **sssd.conf** 文件中的 **ad\_update\_samba\_machine\_account\_password** 选项。在使用 Samba 时轮转机器的域密码时，您可以使用它设置 SSSD 来自动更新 Samba 的 **secrets.tdb** 文件。

但是，如果 SELinux 处于 enforcing 模式，SSSD 无法更新 **secrets.tdb** 文件。因此，Samba 无法访问新密码。要临时解决这个问题，将 SELinux 设置为 permissive 模式。

([BZ#1793727](#))

### SSSD 现在默认强制使用 AD GPOs

SSSD 选项 **ad\_gpo\_access\_control** 的默认设置现在是 **enforcing**。在 RHEL 8 中，SSSD 默认根据活动目录组策略对象(GPO)强制实施访问控制规则。

红帽建议确保在从 RHEL 7 升级到 RHEL 8 前，在 Active Directory 中正确配置 GPO。如果您不想强制执行 GPO，请将 **/etc/sss/sss.conf** 文件中的 **ad\_gpo\_access\_control** 选项的值改为 **permissive**。

([JIRA:RHELPLAN-51289](#))

### 目录服务器现在支持 the pwdReset 操作 属性

此增强为目录服务器增加了对 **pwdReset** 操作属性的支持。当管理员更改用户的密码时，目录服务器在用户的条目中将 **pwdReset** 设为 **true**。因此，应用可以使用此属性来识别管理员是否重置了用户的密码。

请注意，**pwdReset** 是一个操作属性，因此用户无法编辑它。

([BZ#1775285](#))

### 目录服务器现在在 RESULT 条目中记录工作和操作时间



有了这个更新，目录服务器现在在 `/var/log/dirsrv/slapd-<instance_name>/access` 文件的 **RESULT** 的条目中记录两个额外的时间值：

- **wtime** 值指示操作从工作队列移到工作线程所需的时间。
- **optime** 值显示在工作线程启动操作后实际操作完成所花的时间。

新值提供有关 Directory 服务器如何处理负载和进程操作的附加信息。

详情请查看 Red Hat Directory Server Configuration、命令和文件参考中的[访问日志参考部分](#)。

([BZ#1850275](#))

## 5.1.14. Desktop

### 单应用程序会话现在可用

您现在可以在单一应用程序会话中启动 GNOME，也称 kiosk 模式。在这个会话中，GNOME 只显示一个您配置的应用程序的完整屏幕窗口。

启用单一应用程序会话：

1. 安装 **gnome-session-kiosk-session** 软件包：

```
# yum install gnome-session-kiosk-session
```

2. 创建并编辑将打开单应用程序会话的用户的 `$HOME/.local/bin/redhat-kiosk` 文件。在该文件中输入您要启动的应用程序的可执行名称。

例如，启动 **文本编辑器** 应用程序：

```
#!/bin/sh
gedit &
```

3. 使文件可执行：

```
$ chmod +x $HOME/.local/bin/redhat-kiosk
```

4. 在 GNOME 登录屏幕中，从 cogwheel 菜单中选择 **Kiosk** 会话，并作为单一应用程序用户登录。

([BZ#1739556](#))

### tigervnc 被 rebase 到版本 1.10.1

**tigervnc** 套件已 rebase 到版本 1.10.1。该更新包含大量修复及改进。最值得注意的是：

- tigervnc 现在只支持使用 **systemd** 服务管理器启动虚拟网络计算(VNC)服务器。
- 剪贴板现在支持原生 viewer、**WinVNC** 和 Xvnc/libvnc.so 中的完整 Unicode。
- 现在，原生客户端在验证服务器证书时将尊重系统信任存储。
- Java Web 服务器已被删除。
- 现在可将 **x0vncserver** 配置为只允许本地连接。

- **x0vncserver** 在只共享部分显示时会收到修复。
- Polling 现在在 **WinVNC** 中时默认。
- 改进了与 VMware 的 VNC 服务器的兼容性。
- 改进了与 macOS 中一些输入法的兼容性。
- 改进了 JPEG 工件的自动"修复"。

([BZ#1806992](#))

### 5.1.15. 图形基础结构

#### 支持新图形卡

现在完全支持以下图形卡：

- AMD Navi 14 家族, 包括以下模型：
  - Radeon RX 5300
  - Radeon RX 5300 XT
  - Radeon RX 5500
  - Radeon RX 5500 XT
- AMD Renoir APU 家族, 包括以下模型：
  - Ryzen 3 4300U
  - Ryzen 5 4500U、4600U 和 4600H
  - Ryzen 7 4700U、4800U 和 4800H
- AMD Dali APU 家族, 包括以下模型：
  - Athlon Silver 3050U
  - Athlon Gold 3150U
  - Ryzen 3 3250U

另外, 以下图形驱动程序已被更新：

- Matrox **mgag200** 驱动

([JIRA:RHELPLAN-55009](#))

#### 使用 Nvidia Volta 和 Turing 进行硬件加速

**nouveau** 图形驱动程序现在支持使用 Nvidia Volta 和 Turing GPU 家族的硬件加速。因此, 使用 3D 图形的桌面和应用程序现在可以在 GPU 上有效显示。另外, 这可以为其他任务释放 CPU, 并改进整个系统的响应。

([JIRA:RHELPLAN-57564](#))

## 减少 XWayland 的显示测试

XWayland 显示后端现在启用 XPresent 扩展。使用 XPresent，应用程序可以有效地更新其窗口内容，从而减少显示瓶颈。

这个功能显著改进了全屏 OpenGL 应用程序的用户界面,如 3D 编辑器。

(JIRA:RHELPLAN-57567)

## 现在支持 Intel Tiger Lake GPU

在这个版本中，增加了对 Intel Tiger Lake 系列 GPU 的支持。这包括带有以下 CPU 型号的 Intel UHD 图形和 Intel Xe GPU：<https://ark.intel.com/content/www/us/en/ark/products/codename/88759/tiger-lake.html>。

您不再需要设置 `i915.alpha_support=1` 或 `i915.force_probe=*` 内核选项来启用 Tiger Lake GPU 支持。

此增强已作为 [RHSA-2021:0558](#) 异步公告的一部分发布。

(BZ#1882620)

## 5.1.16. Web 控制台

### 从 web 控制台会话中设置权限

在这个版本中，web 控制台提供了一个在管理访问和用户会话内部限制访问之间进行切换的选项。您可以在 web 控制台会话中点击 **Administration access** 或 **Limited access** 指示器来在模式间切换。

(JIRA:RHELPLAN-42395)

### 日志搜索改进

在这个版本中,Web 控制台引入了一个搜索框,支持用户在日志间搜索的一些新方法。搜索框支持日志消息中的正则表达式搜索,指定服务或使用特定日志字段搜索条目。

(BZ#1710731)

### 概述页面显示更详细的 Insights 报告

在这个版本中，当机器连接到 Red Hat Insights 时，Web 控制台的 **Overview** 页面中的 **Health** 卡会显示更多有关点击次数及其优先级的详细信息。

(JIRA:RHELPLAN-42396)

## 5.1.17. Red Hat Enterprise Linux 系统角色

### 为 RHEL 系统角色添加 *Terminal log* 角色

在这个版本中,`rhel-system-roles` 软件包附带的 RHEL 系统角色添加了一个新的 *Terminal log* (TLOG)角色。用户现在可以使用 `tlog` 角色通过 Ansible 来设置和配置会话记录。

目前，`tlog` 角色支持以下任务：

- 配置 `tlog` 以将数据记录到 `systemd` 日志中
- 通过 SSSD 为显式用户和组启用会话记录

(BZ#1822158)

## RHEL Logging 系统角色现在可用于 Ansible

使用日志记录系统角色，您可以在本地和远程主机上部署各种日志记录配置。您可以将 RHEL 主机配置为服务器，以从多个客户端系统中收集日志。

([BZ#1677739](#))

## rhel-system-roles-sap 完全支持

以前作为技术预览提供 **rhel-system-roles-sap** 软件包现已获得全面支持。它为 SAP 提供 Red Hat Enterprise Linux(RHEL)系统角色,可用于自动化 RHEL 系统配置以运行 SAP 工作负载。这些角色通过自动应用基于相关 SAP 备注中最佳实践的优化设置,大大减少了将系统配置为运行 SAP 工作负载的时间。访问只限制为 RHEL for SAP Solutions。如果需要帮助,请联络红帽客户支持团队。

完全支持 **rhel-system-roles-sap** 软件包中的以下新角色：

- **sap-preconfigure**
- **sap-netweaver-preconfigure**
- **sap-hana-preconfigure**

如需更多信息,请参阅 [SAP 的 Red Hat Enterprise Linux 系统角色](#)。

([BZ#1660832](#))

现在,为 Ansible 提供了 **metrics RHEL 系统角色**。

使用 **metrics RHEL 系统角色**,您可以为本地和远程主机配置：

- 通过 **pcp** 应用程序的性能分析服务
- 使用 **grafana** 服务器可视化这些数据
- 使用 **redis** 数据源查询这些数据,而无需手动配置这些服务。

([BZ#1890499](#))

## rhel-system-roles-sap 已升级

**rhel-system-roles-sap** 软件包已升级到上游版本 2.0.0,它提供多个程序错误修复和增强。主要变更包括：

- 改进主机名配置和检查
- 改进 **uuidd** 状态检测和处理
- 添加对 **--check(-c)** 选项的支持
- 将 **nofile** 限制从 32800 增加到 65536
- 在 **sap\_preconfigure\_packages\*** 中添加 **nfs-utils** 文件
- 禁用 **firewalld**。在这个版本中,只在安装了才会禁用 **firewalld**。
- 为 RHEL 8.0 和 RHEL 8.1 添加 **setup** 软件包的最低所需版本。
- 改进 **tmpfiles.d/sap.conf** 文件处理

- 支持单步执行或检查 SAP 备注
- 添加所需 **compat-sap-c++** 软件包
- 改进最小软件包安装处理
- 应用 RHEL 系统角色后，检测是否需要重启
- 支持设置任意 SELinux 状态。默认状态为 **"disabled"**
- 如果多个行具有相同的 IP 地址，则不会再失败
- 如果多个行包含 **sap\_ip**，则不再修改 **/etc/hosts**
- 在 RHEL 7.7 上支持 HANA
- 支持在 **ppc64le** 平台上为 SAP HANA 所需的 IBM 服务和 Power 的生产力工具添加存储库

(BZ#1844190)

### 存储 RHEL 系统角色现在支持文件系统管理

有了这个增强，管理员可以使用 存储 RHEL 系统角色来：

- 调整 **ext4** 文件的大小
- 重新定义 LVM 文件大小
- 使用默认参数在块设备上创建交换分区（如果不存在），或者修改交换分区（如果已存在）。

(BZ#1959289)

## 5.1.18. 虚拟化

### 现在，将虚拟机迁移到不兼容 TSC 设置的主机会失败

在以前的版本中，将虚拟机迁移到带有不兼容时间戳计数器(TSC)设置的主机会在过程后期失败。在这个版本中，尝试这样的迁移会在迁移过程开始前产生一个错误。

(JIRA:RHELPLAN-45950)

### 对第二代 AMD EPYC 处理器的虚拟化支持

在这个版本中。RHEL 8 的虚拟化增加了对第二代 AMD EPYC 处理器的支持，也称 EPYC Rome。因此，在 RHEL 8 中托管的虚拟机现在可以使用 **EPYC-Rome** CPU 模型，并使用处理器提供的新功能。

(JIRA:RHELPLAN-45959)

### 新命令：virsh iothreadset

这个版本引进了 **virsh iothreadset** 命令，可用于配置动态 IOThread 轮询。这样就可以为 I/O 高负载设置虚拟机，从而减少 IOThread 消耗的 CPU 消耗。具体选项请查看 **virsh man page**。

(JIRA:RHELPLAN-45958)

### 目前 KVM 在第 10 代 Intel 核心处理器中支持 UMIP

有了这个更新，KVM 现在支持在第 10 代 Intel Core 处理器（也称为 Ice Lake Server）上运行的主机的用户模式指令预防(UMIP)功能。UMIP 功能会发布一个常规保护意外，当 Current Privilege Level (CPL)

大于 0，特定指令，如 **sgdt**、**sidt**、**sldt**、**smsw** 和 **str** 是否会执行。因此，UMIP 通过防止未经授权应用访问某些系统范围的设置来确保系统安全性，这些设置可用于发起特权升级攻击。

(JIRA:RHELPLAN-45957)

### libvirt 库现在支持 Memory Bandwidth Allocation

**libvirt** 现在支持内存带宽分配(MBA)。使用 MBA,您可以使用 **<cputune>** 部分中的 **<memorytune>** 元素在 vCPU 线程中分配主机内存带宽的部分。

MBA 是 Intel Xeon v4 处理器（也称为 Broadwell 服务器）中现有缓存 QoS 强制(CQE)功能的扩展。对于与 CPU 关联的任务，MBA 使用的机制与 CQE 中使用的相同。

(JIRA:RHELPLAN-45956)

### RHEL 6 虚拟机现在支持 Q35 机器类型

在 RHEL 8 上托管的使用 RHEL 6 作为客户机操作系统的虚拟机(VM)，现在可以使用 Q35，这是一个更加现代的基于 PCI Express 的机器类型。这为虚拟设备的特性和性能提供了各种改进,并确保更广泛的现代设备与 RHEL 6 虚拟机兼容。

(JIRA:RHELPLAN-45952)

**所有日志记录的 QEMU 事件现在都有一个时间戳。因此，用户可以使用保存在 `/var/log/libvirt/qemu/` 目录中的日志更轻松地对虚拟机进行故障排除。**

QEMU 日志现在包含 spice-server 事件的时间戳

在这个版本中，'spice-server' 事件日志添加了时间戳。因此，所有记录的 QEMU 事件现在都有一个时间戳。因此，用户可以使用保存在 `/var/log/libvirt/qemu/` 目录中的日志更轻松地对虚拟机进行故障排除。

(JIRA:RHELPLAN-45945)

### 现在支持 bochs-display 设备

RHEL 8.3 及之后的版本引入了 Bochs 显示设备，其比当前使用的 **stdvga** 设备更安全。请注意，与 **bochs-display** 兼容的所有虚拟机(VM)都将默认使用它。这主要包括使用 UEFI 接口的虚拟机。

(JIRA:RHELPLAN-45939)

### 为虚拟机优化 MDS 保护

有了这个更新，RHEL 8 主机可以通知其虚拟机(VM)它们是否容易受到 [Microarchitectural Data Sampling](#) (MDS)的攻击。不易受攻击的虚拟机不使用 MDS 来提高性能。

(JIRA:RHELPLAN-45937)

### 现在支持在 RBD 中创建 QCOW2 磁盘镜像

在这个版本中，可以在 RADOS Block Device(RBD)存储中创建 QCOW2 磁盘镜像。因此，虚拟机可以使用 QCOW2 镜像来使用 RBD 服务器进行存储后端。

但请注意，在 RBD 存储中 QCOW2 磁盘镜像的写入性能目前低于预期。

(JIRA:RHELPLAN-45936)

### 最大支持的 VFIO 设备增加到 64

在这个版本中，您可以将使用 VFIO 的 64 个 PCI 设备附加到 RHEL 8 主机上的单个虚拟机。RHEL 8.2 及之前的版本为 32。

(JIRA:RHELPLAN-45930)

### 现在 QEMU/KVM 支持 **discard** 和 **write-zeroes** 命令

在这个版本中，QEMU/KVM 支持 **virtio-blk** 的 **discard** 和 **write-zeroes** 命令。因此，虚拟机可以使用 **virtio-blk** 设备丢弃 SSD 中未使用的扇区，并在空闲或者全部填充零扇区。这可用于提高 SSD 性能或确保驱动器安全清除。

(JIRA:RHELPLAN-45926)

### RHEL 8 现在支持 IBM POWER 9 XIVE

这个版本引进了对 IBM POWER9 到 RHEL 8 的 External Interrupt Virtualization Engine (CRCE) 功能的支持。因此，在 IBM POWER 9 系统中的 RHEL 8 管理程序中运行的虚拟机可以使用 XIVE，这会提高 I/O 密集型虚拟机的性能。

(JIRA:RHELPLAN-45922)

### 控制组 v2 虚拟机支持

在这个版本中，libvirt 套件支持控制组 v2。因此，在 RHEL 8 中托管的虚拟机可以利用控制组 v2 的资源控制功能。

(JIRA:RHELPLAN-45920)

### 现在 Windows 虚拟机支持半虚拟 IPI

有了这个更新，**hv\_ipi** 标志已添加到支持的 Windows 虚拟机(VM)的管理程序亮点中。这允许通过超调用发送处理器间中断(IPI)。因此，在运行 Windows OS 的虚拟机上可以更快地执行 IPI。

(JIRA:RHELPLAN-45918)

### 现在可以使用启用磁盘缓存迁移虚拟机

在这个版本中，RHEL 8 KVM 管理程序与磁盘缓存实时迁移兼容。因此，现在可以在启用了磁盘缓存的情况下实时迁移虚拟机。

(JIRA:RHELPLAN-45916)

### 现在非特权会话中的虚拟机可以使用 **macvtap** 接口

现在，虚拟机(VM)可以使用之前由特权进程创建的 **macvtap** 接口。值得注意的是,这可让 **libvirtd** 非特权 **user** 会话启动的虚拟机使用 **macvtap** 界面。

为此，首先在特权环境中创建一个 **macvtap** 接口，并将它设为由将在非特权会话中运行 **libvirtd** 的用户所有。您可以使用 Web 控制台等管理应用程序或者以根用户身份使用命令行实用程序完成此操作，例如：

```
# ip link add link en2 name mymacvtap0 address 52:54:00:11:11:11 type macvtap mode bridge
# chown myuser /dev/tap$(cat /sys/class/net/mymacvtap0/ifindex)
# ip link set mymacvtap0 up
```

之后，修改 VM 的 **<interface>** 配置的 **<target>** 子元素来引用新创建的 **macvtap** 接口：

```
<interface type='ethernet'>
  <model type='virtio'/>
  <mac address='52:54:00:11:11:11'/>
  <target dev='mymacvtap0' managed='no'/>
</interface>
```

使用这个配置时，如果 **libvirt** 以用户 **myuser** 身份运行，VM 会在启动时使用现有的 **macvtap** 界面。

(JIRA:RHELPLAN-45915)

### 虚拟机现在可以使用 Intel 核心处理器 10 代的功能

**Icelake-Server** 和 **Icelake-Client** CPU 模型名称现在可用于虚拟机 (VM)。在有第 10 代 Intel Core 处理器的主机上,使用 **Icelake-Server** 或 **Icelake-Client** 作为虚拟机 XML 配置中的 CPU 类，生成这些 CPU 的新功能，可向虚拟机公开。

(JIRA:RHELPLAN-45911)

### QEMU 现在支持 LUKS 加密

在这个版本中，可以使用 Linux Unified Key Setup(LUKS)加密来创建虚拟磁盘。在创建存储卷时，您可以通过在虚拟机 (VM) XML 配置中包含 **<encryption>** 字段来加密磁盘。您还可以通过在 XML 配置文件中的磁盘域定义中包含 **<encryption>** 字段，让 **LUKS** 加密的虚拟磁盘对虚拟机完全透明。

(JIRA:RHELPLAN-45910)

### 改进了 nbdkit 的日志

**nbdkit** 服务日志记录已被修改为减少冗长。因此，**nbdkit** 只记录潜在的重要信息，**virt-v2v** 转换过程中创建的日志会比较短且更容易解析。

(JIRA:RHELPLAN-45909)

### 提高了虚拟机 SELinux 安全标签和权限的一致性

在这个版本中，**libvirt** 服务可以记录和文件的 SELinux 安全标签和权限，并在修改文件后恢复标签。例如，使用 **libguestfs** 工具修改特定用户拥有的虚拟机 (VM) 磁盘镜像不再将镜像所有者更改为 **root**。

请注意，这个特性不适用于不支持扩展文件属性的文件系统，比如 NFS。

(JIRA:RHELPLAN-45908)

### QEMU 现在在 XTS 密码中使用 gcrypt 程序库

在这个版本中，QEMU 模拟器已被修改为使用 **gcrypt** 库提供的 XTS 密码模式实现。这提高了主机存储使用 QEMU 的原生 **luks** 加密驱动程序的虚拟机的 I/O 性能。

(JIRA:RHELPLAN-45904)

### Windows Virtio 驱动程序现在可以使用 Windows 更新来更新

在这个版本中，QEMU 启动时会默认启动一个新的标准 **SMBIOS** 字符串。**SMBIOS** 字段提供的参数可生成虚拟机上运行的虚拟硬件 ID。因此，Windows Update 可以识别虚拟硬件和 RHEL hypervisor 机器类型，并更新运行 Windows 10+、Windows Server 2016 和 Windows Server 2019+ 的虚拟机上的 Virtio 驱动程序。

(JIRA:RHELPLAN-45901)

### 新命令：virsh guestinfo

在 RHEL 8.3 中引进了 **virsh guestinfo** 命令。这样便可报告有关虚拟机(VM)的以下信息：

- 客户端操作系统和文件系统信息
- 活跃用户



- 使用的时区

运行 **virsh guestinfo** 前，请确定安装了 *qemu-guest-agent* 软件包。另外，VM XML 配置中必须启用 **guest\_agent** 频道，如下所示：

```
<channel type='unix'>
  <target type='virtio' name='org.qemu.guest_agent.0'>
</channel>
```

(JIRA:RHELPLAN-45900)

### KVM 支持用于 BFLOAT16 输入的 VNNI

有了这个更新，支持 **BFLOAT16** 输入（也称为 **AVX512\_BF16** 指令）的 Vector Neural Network Instructions(VNNI)现在也被运行在第 3 代 Intel Xeon 可扩展处理器（也称为 Cooper Lake）上的主机的 KVM 所支持。因此，客户机软件现在可以使用虚拟机内的 **AVX512\_BF16** 指令，方法是在虚拟 CPU 配置中启用它。

(JIRA:RHELPLAN-45899)

### 新命令：virsh pool-capabilities

RHEL 8.3 引进了 **virsh pool-capabilities** 命令选项。此命令显示主机上可用于创建存储池以及每个池中的存储卷的信息。这包括：

- 存储池类型
- 存储池源格式
- 目标存储卷格式类型

(JIRA:RHELPLAN-45884)

### 支持带有 Intel Xeon Platinum 9200 系列处理器的虚拟机中的 CPUID.1F

在这个版本中，在 RHEL 8 中托管的虚拟机可以使用多层的虚拟 CPU 拓扑进行配置，该拓扑使用 Extended Topology Enumeration leaf feature (CPUID.1F)。Intel Xeon Platinum 9200 系列处理器（以前称为 Cascade Lake）支持这个功能。现在，在使用 Intel Xeon Platinum 9200 系列处理器的主机上，可以创建一个带有主机物理 CPU 拓扑的 vCPU 拓扑。

(JIRA:RHELPLAN-37573, JIRA:RHELPLAN-45934)

### 虚拟机现在可以使用 Intel Xeon 可扩展处理器三代功能

**Cooperlake** CPU 模型名称现在可用于虚拟机(VM)。使用 **Cooperlake** 作为虚拟机的 XML 配置中的 CPU 类型，使第三代 Intel Xeon 可扩展处理器的新功能可提供给虚拟机（如果主机使用此 CPU）。

(JIRA:RHELPLAN-37570)

### KVM 现在支持 Intel Optane 持久性内存

在这个版本中，在 RHEL 8 中托管的虚拟机可从 Intel Optane 持久内存技术（之前称为 Intel Crystal Ridge）中受益。Intel Optane 持久内存存储设备提供数据中心级别的持久内存技术，这可以显著提高事务吞吐量。

(JIRA:RHELPLAN-14068)

### 虚拟机现在可以使用 Intel 处理器 Trace

在这个版本中，在 RHEL 8 中托管的虚拟机（VM）可以使用 Intel Processor Trace（PT）功能。当您的主机使用支持 Intel PT 的 CPU 时，您可以使用指定的 Intel 软件来收集有关虚拟机 CPU 性能的各种指标。请注意，这还需要在虚拟机 XML 配置中启用 **intel-pt** 功能。

(JIRA:RHELPLAN-7788)

### DASD 设备现在可以分配给 IBM Z 中的虚拟机

直接访问的存储设备(DASD)提供很多特定的存储功能。使用 **vfio-ccw** 功能，您可以将 DASD 作为中介设备分配给 IBM Z 主机上的虚拟机(VM)。例如，这可以使虚拟机访问 z/OS 数据集，或者与 z/OS 机器共享分配的 DASD。

(JIRA:RHELPLAN-40234)

### IBM Z 支持 IBM Secure Execution

当使用 IBM Z 硬件来运行 RHEL 8 主机时，您可以通过为虚拟机配置 IBM Secure Execution 来提高虚拟机（VM）的安全性。IBM Secure Execution（也称 Protected Virtualization）可防止主机系统访问虚拟机的状态和内存内容。

因此，即使主机被攻击，也无法用作攻击客户端操作系统的向量。另外，安全执行也可以用来防止不可信主机从虚拟机获取敏感信息。

(JIRA:RHELPLAN-14754)

## 5.1.19. 云环境中的 RHEL

### cloud-utils-growpart rebase 为 0.31

**cloud-utils-growpart** 软件包已更新至版本 0.31，它提供多个程序错误修复和增强。主要变更包括：

- 修复了阻止 GPT 磁盘增长过去 2TB 的错误。
- 当启动扇区和大小相同时，**growpart** 操作不再会失败。
- 以前，在一些情况下使用 **sgdisk** 工具重新定义分区大小失败。这个问题现已解决。

([BZ#1846246](#))

## 5.1.20. 容器

### skopeo 容器镜像现已正式发布

**registry.redhat.io/rhel8/skopeo** 容器镜像是 **skopeo** 软件包的容器化实施。**skopeo** 工具是一个命令行工具，可以对容器镜像和镜像存储库执行各种操作。此容器镜像允许您检查 registry 中的容器镜像，从 registry 中移除容器镜像，并将容器镜像从一个未经身份验证的容器 registry 复制到另一个。要拉取 **registry.redhat.io/rhel8/skopeo** 容器镜像，您需要有效的 Red Hat Enterprise Linux 订阅。

([BZ#1627900](#))

### buildah 容器镜像现在可用

**registry.redhat.io/rhel8/buildah** 容器镜像是 **buildah** 软件包的容器化实施。**buildah** 工具可促进构建 OCI 容器镜像。此容器镜像允许您构建容器镜像，而无需在系统中安装 **buildah** 软件包。使用案例不包括在无根模式下作为非 root 用户运行此镜像。要拉取 **registry.redhat.io/rhel8/buildah** 容器镜像，您需要有效的 Red Hat Enterprise Linux 订阅。

([BZ#1627898](#))

## podman v2.0 RESTful API 现已正式发布

新的基于 Podman 2.0 API 的 REST 会根据 varlink 库替换旧的远程 API。新的 API 可在根和无根环境中工作，并提供 docker 兼容层。

(JIRA:RHELPLAN-37517)

## 安装 Podman 不需要 container-selinux

在这个版本中，在容器构建过程中安装 **container-selinux** 软件包是可选的。因此，Podman 对其它软件包的依赖性更少。

(BZ#1806044)

## 5.2. 对外部内核参数的重要更改

本章为系统管理员提供了与 Red Hat Enterprise Linux 8.3 附带的内核有显著变化的总结。这些更改包括添加或更新的 **proc** 条目、**sysctl** 和 **sysfs** 默认值、引导参数、内核配置选项或者任何可见的行为更改。

### 新内核参数

**acpi\_no\_watchdog = [HW,ACPI,WDT]**

启用这个参数来忽略基于 Advanced Configuration 和 Power Interface(ACPI)的 watchdog 接口 (WDAT)，而让原生驱动程序控制 watchdog 设备。

**dfltcc = [HW,S390]**

这个参数配置 IBM Z 构架的 **zlib** 硬件支持。

格式：{ on | off | def\_only | inf\_only | always }

这些选项是：

- **on** (默认) - IBM Z **zlib** 硬件支持一级压缩和解压缩
- **off** - 不支持 IBM Z **zlib** 硬件
- **def\_only** - IBM Z **zlib** 硬件只支持 **deflate** 算法 (级别 1 压缩)
- **inf\_only** - IBM Z **zlib** 硬件只支持 **inflate** 算法 (解压缩)
- **always** - 与 **on** 类似，但会忽略所选的压缩级别，并且始终使用硬件支持 (用于调试)

**irqchip.gicv3\_pseudo\_nmi = [ARM64]**

此参数启用对内核中伪不可屏蔽中断(NMI)的支持。

要使用这个参数，您需要使用 **CONFIG\_ARM64\_PSEUDO\_NMI** 配置项目构建内核。

**panic\_on\_taint =**

使用位掩码来有条件地调用 **add\_taint()** 中的 **panic()**

格式：<hex>[**nousertaint**]

代表一组 **TAINT** 标签的十六进制数字，当使用这个组中的任何标记调用 **add\_taint()** 系统调用时，会导致内核 panic。可选的 **nousertaint** 选项通过将 **panic\_on\_taint** 中的 bitmask 匹配的 flagset 写入 **/proc/sys/kernel/tainted** 文件来防止用户空间强制崩溃。

如需更多信息，请参阅 [上游文档](#)。

**prot\_virt = [S390]**

格式：<bool>

如果硬件支持，此参数允许被保护的虚拟机的托管与 hypervisor 隔离。

**rcutree.use\_softirq = [KNL]**

这个参数启用对 Tree-RCU **softirq** 处理的淘汰。

如果您将此参数设置为零,它会将所有 **RCU\_SOFTIRQ** 进程移动到每个 CPU `rcuc kthreads` 中。如果将 **rcutree.use\_softirq** 设置为非零值 (默认),则默认使用 **RCU\_SOFTIRQ**。指定 **rcutree.use\_softirq=0** 来使用 `rcuc kthreads`。

**split\_lock\_detect = [X86]**

这个参数启用分割锁定检测。启用并存在硬件支持后，访问缓存行边界数据的原子指令将导致协调检查异常。

这些选项是：

- **off** - 未启用
- **warn** - 内核将发出关于触发 Alignment Check Exception(#AC)的应用程序的速率限制警告。这个模式是支持分割锁定检测的 CPU 的默认模式。
- **fatal** - 内核将向触发 #AC 异常的应用程序发送总线错误(SIGBUS)信号。如果在用户模式中遇到了 #AC 异常，而未执行，则内核将在 **warn** 或 **fatal** 模式下发出一个 `oops` 错误。

**srbds = [X86,INTEL]**

这个参数控制特殊寄存器缓冲区数据采样(SRBDS)缓解。

某些 CPU 容易受到类似于 Microarchitectural Data Sampling(MDS)的攻击，该漏洞可能会从随机数字生成器中泄漏位。

默认情况下，`microcode` 可缓解这个问题。但是, `microcode` 修复可能会导致 **RDRAND** 和 **RDSEED** 指令变得非常慢。除其它影响外，这将减少 **urandom** 内核随机源设备吞吐量。

要禁用 `microcode` 缓解方案，请设置以下选项：

- **off** - 禁用缓解方案并消除对 **RDRAND** 和 **RDSEED** 的性能影响

**svm = [PPC]**

格式：{ on | off | y | n | 1 | 0 }

这个参数控制 pSeries 系统中的 Protected Execution Facility 的使用。

**nopv = [X86,XEN,KVM,HYPER\_V,VMWARE]**

此参数禁用 PV 优化功能，它可强制客户端作为无 PV 驱动程序的通用客户端运行。

目前支持 XEN HVM、KVM、HYPER\_V 和 VMWARE 客户端。

**更新的内核参数****hugepagesz = [HW]**

这个参数指定巨页大小。这个参数与 **hugepages** 参数一起使用，预先分配特定大小的巨页。

在对中指定 **hugepagesz** 和 **hugepages** 参数，例如：

```
hugepagesz=2M hugepages=512
```

**hugepagesz** 参数只能在命令行中为特定的巨页面大小指定一次。有效的巨页大小取决于具体的构架。

### hugepages = [HW]

这个参数指定预先分配的巨页数量。这个参数通常遵循有效的 **hugepagesz** 或 **default\_hugepagesz** 参数。

但是，如果 **hugepages** 是第一个或者唯一的 HugeTLB 命令行参数，它将隐式指定要分配的巨页数。如果隐式指定默认大小的巨页数量，则默认大小的 **hugepagesz + hugepages** 参数无法对其进行覆盖。

例如，在有 2M 默认巨页大小的构架中：

```
hugepages=256 hugepagesz=2M hugepages=512
```

从上面示例中的设置结果是分配 256 个 2M 巨页以及一个忽略 **hugepages=512** 参数的警告信息。如果 **hugepages** 之前有无效的 **hugepagesz**，**hugepages** 会被忽略。

### default\_hugepagesz = [HW]

这个参数指定默认的巨页大小。您只能在命令行中指定 **default\_hugepagesz** 一次。另外，您还可以根据 **hugepages** 参数的 **default\_hugepagesz**，来预分配默认大小的一定数量的巨页。另外，您可以隐式指定预分配的默认巨页数量。

例如，在有 2M 默认巨页大小的构架中：

```
hugepages=256
default_hugepagesz=2M hugepages=256
hugepages=256 default_hugepagesz=2M
```

以上示例中的设置会导致分配 256 2M 巨页。有效的默认巨页大小取决于构架。

### efi = [EFI]

格式：{ "old\_map", "nochunk", "noruntime", "debug", "nosoftreserve" }

这些选项是：

- **old\_map** [X86-64] - 切换到旧的基于 ioremap 的 EFI 运行时服务映射。32 位仍默认使用这个
- **nochunk** - 禁止读取 EFI 启动存根的“块”中的文件，因为块可能会导致某些固件实现出现问题
- **noruntime** - 禁用 EFI 运行时服务支持
- **debug** - 启用其他调试输出
- **nosoftreserve** - **EFI\_MEMORY\_SP** (特定用途)属性有时会导致内核为要声明的内存映射驱动程序保留内存范围。指定 **efi=nosoftreserve** 禁用此保留并根据基本类型处理内存（例如 **EFI\_CONVENTIONAL\_MEMORY** / "System RAM"）。

### intel\_iommu = [DMAR]

Intel IOMMU 驱动程序 Direct Memory Access Remapping(DMAR)。

添加的选项有：

- **nobounce** (默认 off) - 对不可信设备（如 Thunderbolt 设备）禁用 bounce 缓冲。这将把不被信任的设备视为可信的设备。因此，此设置可能会暴露直接内存访问(DMA)攻击的安全风险。

**mem = nn[KMG] [KNL,BOOT]**

这个参数强制使用特定数量的内存。

在以下情况下使用的内存量：

1. 用于测试。
2. 当内核无法查看系统内存时。
3. 位于 **mem** 边界后的内存不包括在 hypervisor 中，不会分配给 KVM 客户系统。  
[x86] 以限制最大地址的方式工作。与 **emmap** 参数一起使用以避免物理地址空间冲突。没有 **memmap**，Peripheral Component Interconnect(PCI)设备可以使用属于未使用内存的地址。

请注意，由于上面情况 3 的原因，此设置仅在启动期间生效，如果 hypervisor 的系统内存不够，则可能需要在启动后热添加内存。

**pci = [PCI]**

各种 PCI 子系统选项。

此处的某些选项针对特定的设备或一组设备(<pci\_dev>)而操作。它们使用以下格式之一指定：

```
[<domain>:]<bus>:<dev>.<func>[/<dev>.<func>]*
pci:<vendor>:<device>[:<subvendor>:<subdevice>]
```

请注意，第一种格式指定了 PCI 总线/设备/功能地址，如果主板固件发生了变化，或者因为其他内核参数而导致变化，则该地址在插入新硬件时可能会发生变化。如果未指定域，它将被视为零。另外，通过多个设备/功能地址到设备的路径可以在基础地址后指定（这对于重新编号问题更有效）。第二种格式选择使用 ID 的设备，该配置空间中可能与系统中的多个设备匹配。

这些选项是：

- **hpmiosize** - 为热插拔桥的 Memory-mapped I/O(MMIO)窗口保留的固定总线空间量。默认大小为 2MB。
- **hpmioprefsize** - 为热插拔桥的 MMIO\_PREF 窗口保留的固定总线空间。默认大小为 2MB。

**pcie\_ports = [PCIE]**

外设 Component Interconnect Express(PCIe)端口服务处理。

这些选项是：

- **native** - 使用原生 PCIe 服务（PME、AER、DPC、PCIe 热插拔），即使平台未授予操作系统权限来使用它们。如果平台也尝试使用这些服务，则此设置可能会造成冲突。
- **dpc-native** - 只为 DPC 使用原生 PCIe。如果固件使用 AER 或 93C，则此设置可能会导致冲突。
- **compat** - 禁用原生 PCIe 服务（PME、AER、DPC、PCIe 热插拔）。

**rcu\_nocbs = [KNL]**

参数是一个 CPU 列表。字符串 "all" 可以用来指定系统中的每个 CPU。

**usbcore.authorized\_default = [USB]**

默认 USB 设备授权。

这些选项是：

- **-1**（默认）- 授权，无线 USB 除外

- 0 - 不授权
- 1 - 授权
- 2 - 如果设备连接到内部端口时，授权

`usbcore.old_scheme_first = [USB]`

这个参数允许从旧设备初始化方案开始。这个设置只适用于低速和全速设备（默认值为 0 = off）。

`usbcore.quirks = [USB]`

添加内置 USB 内核 quirk 列表的 quirk 条目列表。列表条目用逗号分开。每个条目的格式为 `VendorID:ProductID:Flags`，例如 `quirks=0781:5580:bk,0a5c:5834:gij`。ID 是 4 位十六进制数，Flags 是一组字母。每个字母都会改变内置的 quirk；如果当前被清除，则设置它，如果当前是设置的，则清除它。

添加的标记：

- 0 - `USB_QUIRK_HUB_SLOW_RESET`，重置端口后，集线器需要额外的延迟

## 新的 /proc/sys/fs 参数

### protected\_fifos

此参数基于 Openwall 软件中的限制，并通过允许避免意外写入攻击者控制的 FIFO 来提供保护，而程序打算在此创建一个常规文件。

这些选项是：

- 0 - 写入 FIFO 是不受限制的。
- 1 - 除非它们归目录的所有者所有，否则不允许对 FIFO 打开 `O_CREAT` 标志，我们在全局可写的粘性目录中并不拥有这些 FIFO。
- 2 - 适用于组可写入粘性目录。

### protected\_regular

这个参数与 `protected_fifos` 参数类似，但它可避免写入攻击者控制的常规文件，而程序打算在此创建一个文件。

这些选项是：

- 0 - 写入常规文件是不受限制的。
- 1 - 除非它们归该目录所有者所有，否则不允许对常规文件打开 `O_CREAT` 标志，我们在全局可写的粘性目录中并不拥有这些常规文件。
- 2 - 适用于组可写入粘性目录。

## 5.3. 设备驱动程序

### 5.3.1. 新驱动程序

#### 网络驱动程序

- CAN driver for Kvaser CAN/USB 设备 (`kvaser_usb.ko.xz`)
- Theobroma Systems UCAN 设备 (`ucan.ko.xz`) 的驱动。

- Pensando 以太网 NIC 驱动程序 (ionic.ko.xz)

### 图形驱动程序和各种驱动程序

- 通用远程处理器框架 (remoteproc.ko.xz)
- Package Level C-state Idle Injection for Intel® CPUs(intel\_powerclamp.ko.xz)
- X86 PKG TEMP Thermal Driver (x86\_pkg\_temp\_thermal.ko.xz)
- INT3402 Thermal driver (int3402\_thermal.ko.xz)
- ACPI INT3403 thermal driver (int3403\_thermal.ko.xz)
- Intel® acpi thermal rel misc dev driver (acpi\_thermal\_rel.ko.xz)
- INT3400 Thermal driver (int3400\_thermal.ko.xz)
- Intel® INT340x common thermal zone handler (int340x\_thermal\_zone.ko.xz)
- Processor Thermal Reporting Device Driver (processor\_thermal\_device.ko.xz)
- Intel® PCH Thermal driver (intel\_pch\_thermal.ko.xz)
- DRM gem ttm helpers (drm\_ttm\_helper.ko.xz)
- Device node registration for cec drivers (cec.ko.xz)
- Fairchild FUSB302 Type-C Chip Driver (fusb302.ko.xz)
- VHOST IOTLB (vhost\_iotlb.ko.xz)
- vDPA-based vhost backend for virtio (vhost\_vdpa.ko.xz)
- VMware virtual PTP clock driver (ptp\_vmw.ko.xz)
- Intel® LPSS PCI driver (intel-lpss-pci.ko.xz)
- Intel® LPSS core driver (intel-lpss.ko.xz)
- Intel® LPSS ACPI driver (intel-lpss-acpi.ko.xz)
- Mellanox watchdog driver (mlx\_wdt.ko.xz)
- Mellanox FAN driver (mlxreg-fan.ko.xz)
- Mellanox regmap I/O access driver (mlxreg-io.ko.xz)
- Intel® speed select interface pci mailbox driver (isst\_if\_mbox\_pci.ko.xz)
- Intel® speed select interface mailbox driver (isst\_if\_mbox\_msr.ko.xz)
- Intel® speed select interface mmio driver (isst\_if\_mmio.ko.xz)
- Mellanox LED regmap driver (leds-mlxreg.ko.xz)
- vDPA Device Simulator (vdpa\_sim.ko.xz)



- Intel® Tiger Lake PCH pinctrl/GPIO driver (pinctrl-tigerlake.ko.xz)
- PXA2xx SSP SPI Controller (spi-pxa2xx-platform.ko.xz)
- CE4100/LPSS PCI-SPI glue code for PXA's driver (spi-pxa2xx-pci.ko.xz)
- Hyper-V PCI Interface (pci-hyperv-intf.ko.xz)
- vDPA bus driver for virtio devices (virtio\_vdpa.ko.xz)

### 5.3.2. 更新的驱动程序

#### 网络驱动程序更新

- VMware vmxnet3 virtual NIC driver (vmxnet3.ko.xz) 已更新到版本 1.5.0.0-k.
- Realtek RTL8152/RTL8153 Based USB Ethernet Adapters(r8152.ko.xz)更新至 1.09.10。
- Broadcom BCM573xx network driver (bnxt\_en.ko.xz) 已更新到版本 1.10.1。
- Netronome Flow Processor (NFP) driver (nfp.ko.xz) 已更新到版本 4.18.0-240.el8.x86\_64.
- Intel® Ethernet Switch Host Interface Driver(fm10k.ko.xz)更新至 0.27.1-k 版本。
- Intel® Ethernet Connection E800 Series Linux Driver(ice.ko.xz)更新至版本 0.8.2-k。

#### 存储驱动程序更新

- Emulex LightPulse Fibre Channel SCSI 驱动程序(lpfc.ko.xz)更新至版本 0:12.8.0.1。
- QLogic FCoE Driver(bnx2fc.ko.xz)更新至 2.12.13 版本。
- LSI MPT Fusion SAS 3.0 Device Driver(mpt3sas.ko.xz)更新至34.100.00.00。
- HP Smart Array Controller 版本(hpsa.ko.xz)的驱动已更新至版本 3.4.20-170-RH5。
- QLogic Fibre Channel HBA Driver(qla2xxx.ko.xz)更新至 10.01.00.25.08.3-k。
- Broadcom MegaRAID SAS Driver(megaraid\_sas.ko.xz)已更新至版本 07.714.04.00-rh1。

#### 图形和各种驱动程序更新

- VMware SVGA 设备(vmwgfx.ko.xz)的独立 drm 驱动程序已更新至 2.17.0.0 版本。
- Chelsio Terminator 卡的加密 Co-processor 已更新至版本 1.0.0.0-ko。

## 5.4. 程序错误修复

这部分论述了 Red Hat Enterprise Linux 8.3 中修复的、对用户有严重影响的错误。

### 5.4.1. 安装程序和镜像创建

#### RHEL 8 初始设置现在可以通过 SSH 正常工作

在以前的版本中，当使用 SSH 登录到系统时，RHEL 8 初始设置接口不会显示。因此，无法在通过 SSH 管理的 RHEL 8 机器上执行初始设置。这个问题已被解决，在通过 SSH 进行时，RHEL 8 初始设置现在可以正常工作。

(BZ#1676439)

### 使用 `reboot --kexec` 命令安装失败

在以前的版本中，当使用包含 `reboot --kexec` 命令的 Kickstart 文件时，RHEL 8 安装会失败。

在这个版本中，`reboot --kexec` 的安装可以正常工作。

(BZ#1672405)

### America/New York 时区现在可以正确设置

在以前的版本中，交互式 Anaconda 安装过程不允许用户在使用 kickstart 文件设置 *America/New York* 时区。在这个版本中，如果在 kickstart 文件中没有指定时区，用户现在可以将 *America/New York* 设定为互动安装程序的首选时区。

(BZ#1665428)

### 现在正确设置了 SELinux 环境

在以前的版本中，当 SELinux 处于 enforcing 模式时，某些文件夹和文件中的 SELinux 上下文不正确，从而导致在安装后试图访问这些文件时出现意外的 AVC 拒绝。

在这个版本中，Anaconda 会设置正确的 SELinux 上下文。现在，您可以在不手动重新标记文件系统的情况下访问文件夹和文件。

(BZ#1775975)

### 自动分区现在创建有效的 /boot 分区

在以前的版本中，当使用自动分区或使用带有预配置分区的 kickstart 文件的系统中安装 RHEL 时，安装程序会创建一个可能包含无效的 /boot 分区的分区方案。因此，因为分区方案验证失败，自动安装过程被提前失败。在这个版本中，Anaconda 会创建一个包含有效 /boot 分区的分区方案。因此，自动安装可以如预期完成。

(BZ#1630299)

### 使用 Binary DVD ISO 镜像的 GUI 安装现在可以成功完成，无需 CDN 注册

在以前的版本中，当使用 Binary DVD ISO 镜像文件执行 GUI 安装时，安装程序的一个竞争条件会阻止安装，直到您使用连接到红帽功能注册系统为止。

在这个版本中，您可以继续安装，而不必使用连接到红帽的功能注册该系统。

(BZ#1823578)

### 在 Kickstart 中创建并在 `ignoredisk --only-use` 命令中使用的 iSCSI 或者 FCoE 设备不再停止安装进程

在以前的版本中，当 `ignoredisk --only-use` 命令中使用的在 Kickstart 中创建的 iSCSI 或 FCoE 设备时，安装程序会失败，并显示与 `Disk "disk/by-id/scsi-360a9800042566643352b476d674a774a" given in ignoredisk command does not exist` 类似的错误。这会停止安装进程。

在这个版本中，这个问题已被解决。安装程序继续工作。

(BZ#1644662)

### 使用 CDN 的系统注册失败并显示错误 `Name or service not known`

当您尝试使用内容交付网络(CDN)注册系统时，注册过程会失败，并显示错误消息 **Name or service not known**。

出现这个问题的原因是，空 **Custom server URL** 和 **Custom Base URL** 值覆盖系统注册的默认值。

在这个版本中，空值不会覆盖默认值，系统注册可以成功完成。

(BZ#1862116)

## 5.4.2. 软件管理

### **dnf-automatic** 现在只更新正确 GPG 签名的软件包

在以前的版本中，在执行更新前，**dnf-automatic** 配置文件不会检查下载的软件包的 GPG 签名。因此，非导入密钥的未签名更新或更新可能会被 **dnf-automatic** 安装，即使存储库配置需要 GPG 签名检查 (**gpgcheck=1**)。在这个版本中，这个问题已被解决，**dnf-auto** 在执行更新前会检查下载的软件包的 GPG 签名。因此，只有使用正确 GPG 签名的更新才可以从需要 GPG 签名检查的库中安装。

(BZ#1793298)

### 逗号不再导致在 **append** 类型选项中删除条目

在以前的版本中，在 **append** 类型选项（如 **exclude**、**excludepkgs**、**includepkgs**）中添加结尾的逗号（在列表末尾的一个空条目）会导致删除选项中的所有条目。另外，添加两个逗号（一个空条目）会导致仅在逗号后的条目被使用。

在这个版本中，会忽略不是前导逗号（前导逗号代表列表以一个空条目开始）的空条目。因此，只有开头的逗号从 **append** 类型选项中删除现有的条目，用户可以使用它来覆盖这些条目。

(BZ#1788154)

## 5.4.3. Shell 和命令行工具

### **ReaR** 磁盘布局不再包含 Rancher 2 Longhorn iSCSI 设备和文件系统的条目

这个版本从 **ReaR** 创建的磁盘布局中删除 Rancher 2 Longhorn iSCSI 设备以及文件系统条目。

(BZ#1843809)

### 现在在 IBM POWER, little endian 上启用一个大于 4 GB 文件的救援镜像创建

在以前的版本中，**ReaR** 工具无法创建包含在 IBM POWER, little endian 架构中大于 4GB 的救援镜像。在这个版本中，这个问题已被解决，现在可以在 IBM POWER, little endian 上创建一个大于 4 GB 的文件。

(BZ#1729502)

## 5.4.4. 安全性

### SELinux 不再阻止 **systemd-journal-gatewayd** 在 **/dev/shm/ corosync** 中使用 **newfstatat()** 调用

在以前的版本中，SELinux 策略不包含一个允许 **systemd-journal-gatewayd** 守护进程访问由 **corosync** 服务创建的文件的规则。结果是 SELinux 会拒绝 **systemd-journal-gatewayd** 调用在由 **corosync** 创建的共享内存文件中调用 **newfstatat()** 功能。在这个版本中，SELinux 不再阻止 **systemd-journal-gatewayd** 在 **corosync** 创建的共享内存文件中调用 **newfstatat()**。

(BZ#1746398)

## libreswan 现在在所有配置上与 seccomp=enabled 一起工作

在这个更新之前，Libreswan SECCOMP 支持实现中允许的一组系统调用与 RHEL 库的新用法不匹配。因此，当 `ipsec.conf` 文件中启用了 SECCOMP，`syscall` 会过滤拒绝的事件 `syscalls`，而 `pluto` 守护进程需要它；守护进程会被终止，`ipsec` 服务被重启。在这个版本中，所有新必需的 `syscalls` 都被允许，Libreswan 现在可以和 `seccomp=enabled` 选项一起正常工作。

(BZ#1544463)

## SELinux 不再阻止 auditd 停止或者关闭系统

在以前的版本中，SELinux 策略不包含一个允许 Audit 守护进程启动 `power_unit_file_t systemd` 单元的规则。因此，在日志磁盘分区没有剩余空间的情况下，`auditd` 也无法停止或关闭系统。

这个 `selinux-policy` 软件包的更新添加了缺少的规则，现在 `auditd` 可以正确地停止并关闭系统，且只能在 enforcing 模式的 SELinux 下关闭系统。

(BZ#1826788)

## IPTABLES\_SAVE\_ON\_STOP 现在可以正常工作

在以前的版本中，`iptables` 服务的 `IPTABLES_SAVE_ON_STOP` 功能无法正常工作，因为保存的 IP 表内容的文件接收到不正确的 SELinux 上下文。这导致 `iptables` 脚本无法更改权限，因此该脚本无法保存更改。这个版本为 `iptables.save` 和 `ip6tables.save` 文件定义了正确的上下文，并创建了文件名转换规则。因此，`iptables` 服务的 `IPTABLES_SAVE_ON_STOP` 功能可以正常工作。

(BZ#1776873)

## NSCD 数据库现在可以使用不同的模式

`nsswitch_domain` 属性中的域被允许访问 Name Service Cache Daemon(NSCD)服务。每个 NSCD 数据库都在 `nscd.conf` 文件中配置，且 `shared` 属性决定数据库是使用 Shared memory 还是 Socket 模式。在以前的版本中，所有 NSCD 数据库都必须使用相同的访问模式，这取决于 `nscd_use_shm` 布尔值。现在，总是允许使用 Unix 流套接字，因此不同的 NSCD 数据库可以使用不同的模式。

(BZ#1772852)

## 当使用 --sudo 扫描远程系统时，oscap-ssh 工具现在可以正常工作

在使用带有 `--sudo` 选项的 `oscap-ssh` 工具对远程系统执行安全内容自动化协议(SCAP)扫描时，远程系统上的 `oscap` 工具以 `root` 用户的身份将扫描结果和报告文件保存到一个临时目录中。在以前的版本中，如果远程机器中的 `umask` 设置被改变，`oscap-ssh` 可能会无法访问这些文件。在这个版本中解决了这个问题，`oscap` 以目标用户身份保存文件，而 `oscap-ssh` 会正常访问这些文件。

(BZ#1803116)

## OpenSCAP 现在正确处理远程文件系统

在以前的版本中，如果挂载规范没有以两个斜杠开头，OpenSCAP 将无法可靠地检测远程文件系统。因此，OpenSCAP 将一些基于网络的文件系统作为本地文件系统进行处理。有了这个更新，OpenSCAP 使用文件系统类型而不是挂载规范来识别文件系统。因此，OpenSCAP 现在可以正确处理远程文件系统。

(BZ#1870087)

## openscap 不再从 YAML 多行字符串中删除空白行

在以前的版本中，OpenSCAP 会从数据流生成的 Ansible 修复中删除 YAML 多行字符串中的空白行。这会影响 Ansible 修复，并导致 `openscap` 工具未能通过响应的开放漏洞和评估语言(OVAL)检查，从而产生假阳性结果。这个问题现已解决，因此 `openscap` 不再从 YAML 多行字符串中删除空白行。

[\(BZ#1795563\)](#)

### OpenSCAP 现在可以在没有内存不足的情况下扫描含有大量文件的系统

在以前的版本中，当扫描内存较低和大量文件的系统时，OpenSCAP 扫描程序有时会导致系统内存不足。在这个版本中，OpenSCAP 扫描程序内存管理有所改进。因此，扫描程序在扫描大量文件时，如，软件包组 **Server with GUI** 和 **Workstation**，在 RAM 较少的系统上不会再耗尽内存。

[\(BZ#1824152\)](#)

### config.enabled 现在可以正确地控制语句

在以前的版本中，**rsyslog** 在语句的配置处理过程中错误地评估了 **config.enabled** 指令。因此，对于除了 **include()** 外的每一个语句，都会显示 **parameter not known** 错误。在这个版本中，所有语句都会相等地处理。现在，**config.enabled** 可以正确地禁用或启用语句而无需显示任何错误。

[\(BZ#1659383\)](#)

### fapolicyd 不再阻止 RHEL 更新

当更新替换了正在运行的应用程序的二进制文件时，内核会通过附加 "(deleted)" 后缀来修改内存中的应用程序二进制路径。在以前的版本中，**fapolicyd** 文件访问策略守护进程将此类应用程序视为不受信任的应用程序，并阻止它们打开和执行任何其他文件。因此，在应用更新后系统有时无法启动。

随着 [RHBA-2020:5242](#) 公告的发布，**fapolicyd** 会忽略二进制路径中的后缀，以便二进制文件可以匹配信任的数据库。因此，**fapolicyd** 会正确强制执行规则，并使更新过程可以完成。

[\(BZ#1897090\)](#)

### e8 配置文件现在可以用来修复带有 Server with GUI 的 RHEL 8 系统

使用 OpenSCAP Anaconda 附加组件强化带有配置文件的 **Server with GUI** 软件包组上的系统，该配置文件从 **Verify Integrity with RPM** 组中选择规则，不再需要系统上大量的 RAM。造成此问题的原因是 OpenSCAP 扫描程序。如需了解更多详细信息，请参阅[扫描大量使用 OpenSCAP 的文件会导致系统内存不足](#)。因此，使用 RHEL 8 Essential Eight(e8)配置文件强化系统现在也可以使用 **Server with GUI**。

[\(BZ#1816199\)](#)

## 5.4.5. 网络

### nft\_compat 模块自动加载 iptables 扩展模块不再挂起

在以前的版本中，当 **nft\_compat** 模块加载一个扩展模块，而网络命名空间(**netns**)操作并行发生时，如果该扩展在初始化过程中注册了一个 **pernet** 子系统，则会发生锁冲突。因此，内核调用的 **modprobe** 命令会挂起。这也可能是由其它还执行 **iptables** 命令的服务（比如 **libvirtd**）造成。这个问题已被解决。因此，由 **nft\_compat** 模块载入 **iptables** 扩展模块不再挂起。

[\(BZ#1757933\)](#)

### 现在，firewalld 服务在服务停止时删除 ipset

在以前的版本中，停止 **firewalld** 服务不会删除 **ipset**。在这个版本中解决了这个问题。因此，**firewalld** 停止后 **ipset** 不再会留在系统中。

[\(BZ#1790948\)](#)

### firewalld 在关闭后不再保留 ipset 条目

在以前的版本中，关闭 **firewalld** 不会删除 **ipset** 条目。因此，**ipset** 条目即使在停止 **firewalld** 服务后仍保留在内核中。在这个版本中，关闭 **firewalld** 会如预期删除 **ipset** 条目。

(BZ#1682913)

### **firewalld** 现在在重新载入后恢复 **ipset** 条目

在以前的版本中，**firewalld** 在重新载入后无法保留运行时 **ipset** 条目。因此，用户需要手动添加缺少的条目。在这个版本中，**firewalld** 已被修改来在重新加载后恢复 **ipset** 条目。

(BZ#1809225)

### **nftables** 和 **firewalld** 服务现在是相互排斥的

在以前的版本中，您可以同时启用 **nftables** 和 **firewalld** 服务。因此，**nftables** 会覆盖 **firewalld** 规则集。在这个版本中，**nftables** 和 **firewalld** 服务是相互排斥的，因此无法同时启用它们。

(BZ#1817205)

## 5.4.6. 内核

### **huge\_page\_setup\_helper.py** 脚本现在可以正常工作

更新 Python 3 的 **huge\_page\_setup\_helper.py** 脚本的补丁被意外删除。因此，在执行 **huge\_page\_setup\_helper.py** 后会出现以下错误信息：

```
SyntaxError: Missing parentheses in call to 'print'
```

有了这个更新，这个问题已通过更新 **libhugetlbfs.spec** 文件解决了。因此，**huge\_page\_setup\_helper.py** 在描述的场景中不会显示任何错误。

(BZ#1823398)

### 有大量持久内存的系统启动更快，且不会超时

有大量持久内存的系统需要很长时间才能启动，因为初始源代码只允许每个节点有一个初始化线程。例如，对于 4 节点系统，有 4 个内存初始化线程。因此，如果 **/etc/fstab** 文件中列出了持久内存文件系统，则系统在等待设备可用时可能会超时。有了这个更新，这个问题已被解决，因为源代码现在允许单个节点中有多个内存初始化线程。因此，系统启动会更快，在上述场景中没有出现超时。

(BZ#1666538)

### **bcc** 脚本现在可以成功编译 BPF 模块

在编译脚本代码以创建 Berkeley Packet Filter(BPF)模块期间，**bcc** 工具包对数据类型定义使用内核头文件。有些内核标头需要定义 **KBUILD\_MODNAME** 宏。因此，那些没有添加 **KBUILD\_MODNAME** 的 **bcc** 脚本可能无法在不同的 CPU 构架中编译 BPF 模块。以下 **bcc** 脚本会受到影响：

- **bindsnoop**
- **sofdsnoop**
- **solisten**
- **tcpaccept**
- **tcpconnect**

- `tcpconnl`
- `tcpdrop`
- `tcpretrans`
- `tcpsubnet`
- `tcptop`
- `tcptracer`

在这个版本中,把 `KBUILD_MODNAME` 添加到 `bcc` 的默认 `cflags` 参数解决了这个问题。因此,这个问题不再出现在上述场景中。另外,客户脚本也不需要自行定义 `KBUILD_MODNAME`。

(BZ#1837906)

**`bcc-tools` 和 `bpfftrace` 可以在 IBM Z 上正常工作。**

在以前的版本中,包括一个 `ARCH_HAS_NON_OVERLAPPING_ADDRESS_SPACE` 内核选项。然而,IBM Z 构架的 `bcc-tools` 软件包和 `bpfftrace` 追踪语言没有对这个选项的适当支持。因此,`bpf()` 系统调用失败,并显示 `Invalid 参数` 异常,`bpfftrace` 失败,并在尝试载入 BPF 程序时给出 `Error loading program` 程序错误。在这个版本中,`ARCH_HAS_NON_OVERLAPPING_ADDRESS_SPACE` 选项被删除。因此,这个问题不再出现在上述场景中。

(BZ#1847837, BZ#1853964)

**不再会因为缺少熵导致引导过程失败**

在以前的版本中,会因为缺少熵引导过程失败。现在,使用一种更好的机制来允许内核在引导过程早期收集熵,这不依赖于任何特定的硬件中断。在这个版本中,确保有足够的熵来保证早期引导时随机生成安全,从而解决了这个问题。在这个版本中,可以防止 `kickstart` 超时或者引导速度慢,引导过程可以正常工作。

(BZ#1778762)

**使用 `kexec` 重复重启现在如预期正常工作**

在以前的版本中,内核在 Amazon EC2 Nitro 平台上重启过程中,在内核执行路径的 `shutdown ()` 调用过程中不会调用删除模块(`rmmmod`)。因此,使用 `kexec` 系统调用重复内核重启会导致失败。有了这个更新,问题已通过添加允许安全内核执行的 `PCI shutdown ()` 处理程序解决了。因此,在 Amazon EC2 Nitro 平台上重复使用 `kexec` 重启不再会失败。

(BZ#1758323)

**使用 `vPMEM` 内存重启作为转储目标现在可以正常工作**

在以前的版本中,使用虚拟持久内存(`vPMEM`)命名空间作为 `kdump` 或 `fadump` 的转储目标导致了 `papr_scm` 模块取消和重新映射由 `vPMEM` 支持的内存,并将内存重新添加到其线性映射中。

因此,这个行为触发了对 POWER Hypervisor 的 Hypervisor 调用(HCalls)。因此,这会大大减慢捕获内核引导的速度,并需要很长时间来保存转储文件。在这个版本中解决了这个问题,引导过程可以正常工作。

(BZ#1792125)

**尝试将 `ICE` 驱动程序 NIC 端口添加到模式 5 bonding master 接口不再失败**

在以前的版本中,试图将 `ICE` 驱动程序 NIC 端口添加到模式 5 (`balance-tlb`)绑定 master 接口会导致一个错误 `Master 'bond0',Slave 'ens1f0': Error: Enslave failed`。因此,会出现将 NIC 端口添加到绑定 master 接口中断失败的问题。在这个版本中解决了这个问题,添加接口不会失败。

(BZ#1791664)

### cxgb4 驱动程序不再导致 kdump 内核崩溃

在以前的版本中，在尝试在 **vmcore** 文件中保存信息的过程中，**kdump** 内核会崩溃。因此，**cxgb4** 驱动程序会阻止 **kdump** 内核保存为以后进行分析的内核。要临时解决这个问题，在 **kdump** 内核命令行中添加 **novmcoredd** 参数以允许保存内核文件。

随着 [RHSA-2020:1769](#) 公告的发布，**kdump** 内核可以正确处理这种情况，不再崩溃。

(BZ#1708456)

## 5.4.7. 高可用性和集群

### 当在 Filesystem 代理中使用 GFS2 文件系统时, fast\_stop 选项现在默认为 no

在以前的版本中，当与 Filesystem 代理一起使用 GFS2 文件系统时，**fast\_stop** 选项默认为 **yes**。这个值可能会导致不必要的保护事件，因为 GFS2 文件系统可能需要较长时间卸载。在这个版本中，这个选项被默认为 **no**。对于所有其他文件系统，默认为 **yes**。

(BZ#1814896)

### fence\_compute 和 fence\_evacuate 代理现在以更标准的方式解释 insecure 选项

在以前的版本中，**fence\_compute** 和 **fence\_evacuate** 代理可以正常工作，就像默认指定 **--insecure** 一样。在这个版本中，没有为 **compute** 或 **evacuate** 服务使用有效证书时，需要设置 **insecure=true**，并在通过 CLI 手动运行时使用 **--insecure** 选项。这与所有其他代理的行为一致。

(BZ#1830776)

## 5.4.8. 动态编程语言、网页和数据库服务器

### 通过 libdb 优化 CPU 的使用

在以前的版本中对 **libdb** 数据库的更新会过度消耗 CPU。在这个版本中，CPU 的使用已被优化。

(BZ#1670768)

### did\_you\_mean Ruby gem 不会包括一个带有非商用许可证的文件。

在以前的版本中，**did\_you\_mean** gem 包括在带有非商用许可证文件的 **ruby:2.5** 模块流中。在这个版本中，删除了受影响的文件。

(BZ#1846113)

### nginx 现在可以通过 PKCS#11 URI 从硬件安全令牌加载服务器证书

**nginx** web 服务器的 **ssl\_certificate** 指令支持直接从 PKCS#11 模块的硬件安全令牌加载 TLS 服务器证书。在以前的版本中，无法通过 PKCS#11 URI 从硬件安全令牌加载服务器证书。

(BZ#1668717)

## 5.4.9. 编译器和开发工具

### 当加载使用 DT\_FILTER 并有一个构造器的共享库时, glibc 动态加载程序不再会失败

在这个更新之前，**glibc** 构造器的共享库的动态加载程序实现中的一个缺陷导致了动态加载程序在加载时



在这个更新之前，作为过滤器的共享对象的动态加载程序实现中的一个缺陷导致了动态加载程序在加载使用过滤器并有一个构造器的共享库时失败。有了这个版本，过滤器的动态加载程序实现(DT\_FILTER)已被修复，能够正确处理此类共享库。因此，在上面提到的场景中，这个动态装载程序可以正常工作。

(BZ#1812756)

### glibc 现在可以从 getmntent () 列表中删除伪挂载

内核在向用户空间公开的表格中包括 **automount** 伪条目。因此，使用 **getmntent()** API 的程序会在列表中看到常规挂载和这些伪挂载。pseudo-mounts 与实际装载不对应,也不包含有效信息。

在这个版本中,如果挂载条目在 **automount (8)** 配置中有 **ignore** 挂载选项，**glibc** 库现在会从 **getmntent()** 列表中删除这些伪挂载。预期前面的行为的程序必须使用不同的 API。

(BZ#1743445)

### movv1qi 模式不再会在 IBM Z 的自动验证代码中造成错误。

在以前的版本中，**movv1qi** 模式给出错误的加载指令。因此，当自动vectorization 生效时，可能会在 IBM Z 系统中出现错误。在这个版本中解决了 **movv1qi** 模式的问题，因此代码可以被编译并正常运行。

(BZ#1784758)

### PAPI\_event\_name\_to\_code() 现在可以在多个线程中正常工作

在以前的版本中，PAPI 内部代码无法正确处理线程协调。因此,当多个线程使用 **PAPI\_event\_name\_to\_code()** 操作时，竞争条件发生，操作会失败。这个版本改进了对 PAPI 内部代码中多个线程的处理。因此，使用 **PAPI\_event\_name\_to\_code()** 操作的多线程代码现在可以正常工作。

(BZ#1807346)

### 提高了 IBM Power 系统上的 glibc 数学功能的性能

在以前的版本中，**glibc** 数学函数在 IBM Power Systems 上执行不必要的浮点状态更新和系统调用，这对性能造成了负面影响。这个版本删除了不必要的浮动点状态更新,并改进了以下的实现 **ceil()**, **ceilf()**, **fegetmode()**, **fesetmode()**, **fesetenv()**, **fegetexcept()**, **feenableexcept()**, **fedisableexcept()**, **fegetround()** and **fesetround()**。因此, math 库的性能在 IBM Power Systems 上都有改进。

(BZ#1783303)

### 现在 IBM Power 支持内存保护密钥

在 IBM Power 系统上，内存保护密钥接口 **pkey\_set** 和 **pkey\_get** 之前是 stub 功能，因此会失败。这个更新实现了接口，因此，GNU C 库(**glibc**)现在在 IBM Power 系统上支持内存保护密钥。

请注意，内存保护密钥目前需要基于哈希的内存管理单元(MMU)，因此您可能需要使用 **disable\_radix** 内核参数启动某些系统。

(BZ#1642150)

### Papi-testsuite 和 papi-devel 现在安装所需的 papi-libs 软件包

在以前的版本中，**papi-testsuite** 和 **papi-devel** RPM 软件包没有声明依赖匹配的 **papi-libs** 软件包。因此，测试无法运行，开发人员没有为其应用程序提供的 **papi** 共享库所需的版本。

在这个版本中，当用户安装 **papi-testsuite** 或 **papi-devel** 软件包时，还会安装 **papi-libs** 软件包。因此，**papi-testsuite** 现在有允许测试运行的正确的库，使用 **papi-devel** 的开发人员将其可执行文件与适当的 **papi** 共享库版本进行连接。

[\(BZ#1664056\)](#)

### 为多个构架安装 `lldb` 软件包不再会导致文件冲突

之前，`lldb` 软件包在架构独立位置安装与构架相关的文件。因此，在 32 位和 64 位版本中安装软件包会导致文件冲突。这个更新会将文件打包成正确的体系独立位置。因此，在以上场景中安装 `lldb` 可以成功完成。

[\(BZ#1841073\)](#)

### `getaddrinfo` 现在可以正确地处理内存分配失败

之前，在内存分配失败后，GNU C 库 `glibc` 的 `getaddrinfo` 功能不会释放内部解析器上下文。因此，`getaddrinfo` 无法在调用线程的剩余生命周期内重新载入 `/etc/resolv.conf` 文件，从而导致内存泄漏。

这个版本使用解析程序上下文的额外发行版本操作修改错误处理路径。因此，`getaddrinfo` 会根据新的配置值重新载入 `/etc/resolv.conf`，即使内存分配失败也是如此。

[\(BZ#1810146\)](#)

### `glibc` 避免了 IFUNC 解析顺序导致的某些故障

之前，GNU C 库 `glibc` 的 `librt` 和 `libpthread` 库的实现包含以下功能的间接功能(IFUNC)解析程序：`clock_gettime`、`clock_getcpuclockid`、`clock_nanosleep`、`clock_settime`、`vfork`。在某些情况下，IFUNC 解析器可以在 `librt` 和 `libpthread` 库被重新定位前执行。因此，在早期程序启动时，应用程序会在 `glibc` 动态加载程序中失败。

在这个版本中，这些功能的实现被移到 `glibc` 的 `libc` 组件中，这可以防止上面描述的问题发生。

[\(BZ#1748197\)](#)

### 在 `pthread_create` 过程中不再发生伪装失败

在以前的版本中，`glibc` 动态加载程序不会回滚对内部线程本地存储(TLS)模块 ID 计数器的更改。因此，`dlopen` 功能在某些方面失败后，`pthread_create` 函数中的错误可能会发生。在这个版本中，`glibc` 动态加载程序会在特定故障无法再发生时更新 TLS 模块 ID 计数器。因此，不会再出现问题。

[\(BZ#1774115\)](#)

### `glibc` 现在使用 `nss_db` 为 32 位应用程序安装正确的依赖软件包

在以前的版本中，`nss_db.x86_64` 软件包没有声明依赖 `nss_db.i686` 软件包。因此，自动安装不会在系统中安装 `nss_db.i686`，尽管安装了 32 位环境 `glibc.i686`。因此，使用 `nss_db` 的 32 位应用程序无法执行准确的用户数据库查找，而同时设置的 64 位应用程序可以正常工作。

在这个版本中，`glibc` 软件包现在有弱的依赖关系，在 `glibc.i686` 和 `nss_db` 都在系统上安装时，会触发 `nss_db.i686` 软件包的安装。因此，使用 `nss_db` 的 32 位应用程序现在可以正常工作，即使系统管理员还没有显式安装 `nss_db.i686` 软件包。

[\(BZ#1807824\)](#)

### 使用 Odia 语言更新的 `glibc` 语言信息

以前称为 Orissa 的印度州已改为 Odisha，其官方语言的名称已从 Oriya 改为 Odia。在这个版本中，`glibc` 区域信息会显示语言的新名称。

[\(BZ#1757354\)](#)

## LLVM 子软件包现在在与架构相关的位置安装 arch-dependent 文件

在以前的版本中，LLVM 子软件包在 arch 独立位置安装 arch-dependent 文件。这会导致在安装 32 和 64 位 LLVM 版本时出现冲突。在这个版本中，软件包文件可以被正确地安装在与架构相关的位置，从而避免了版本冲突。

(BZ#1820319)

## 密码和组查找在 glibc 中不再失败

在以前的版本中，在处理密码和组条目时，glibc 库的 nss\_compat 模块会用错误的代码覆盖 errno 状态。因此，应用程序不会按预期调整缓冲区的大小，从而导致密码和组查找失败。这个更新解决了这个问题，现在查找可以按预期完成。

(BZ#1836867)

## 5.4.10. Identity Management

### SSSD 不再默认下载带有通配符字符的每个规则

在以前的版本中，默认情况下 ldap\_sudo\_include\_regexp 选项被错误地设定为 true。当 SSSD 运行或者更新 SSSD 规则后，SSSD 会下载 sudoHost 属性中包含通配符字符(\*)的所有规则。这个更新解决了 bug，ldap\_sudo\_include\_regexp 选项默认会被正确设置为 false。因此，上面描述的问题不再发生。

(BZ#1827615)

### krb5 现在是唯一需要的加密类型

在以前的版本中，如果没有设置 default\_tgs\_etypes 或 default\_tkt\_etypes 属性，在 /etc/krb5.conf 文件中的 permitted\_etypes 变量指定的允许的加密类型不会应用到默认的加密类型。因此，Kerberos 客户端可以请求已弃用的密码套件，如 RC4，这可能会导致其他进程失败。有了这个更新，permitted\_etypes 变量中指定的加密类型也会应用到默认的加密类型，并且只请求允许的加密类型。

RC4 密码套件已在 RHEL 8 中被弃用，其是 AD 林中活动目录(AD)域之间用户、服务和信任的默认加密类型。

- 要确保在 AD 林中 AD 域之间支持强 AES 加密类型，请参阅 [AD DS: 安全: 当访问信任域中的资源时](#)，Kerberos "Unsupported etype" 错误的微软文章
- 要启用对 IdM 服务器中已弃用的 RC4 加密类型的支持，以便与 AD 兼容，请使用 `update-crypto-policies --set DEFAULT:AD-SUPPORT` 命令。

(BZ#1791062)

### KDC 现在从 LDAP 后端正确强制执行密码生命周期策略

在以前的版本中，非 IPA Kerberos 分发中心(KDC)无法确保最大密码生存期，因为 Kerberos LDAP 后端错误地强制执行密码策略。在这个版本中，Kerberos LDAP 后端已被修复，密码生命周期可以正常工作。

(BZ#1784655)

### 使用 SSSD 发送到 AD 客户端的密码过期通知

在以前的版本中，使用 SSSD 的 Active Directory 客户端（非 IdM）不会发送密码过期通知，因为 SSSD 界面最近更改了获取 Kerberos 凭证。

Kerberos 界面已更新,现在正确发送过期通知。

[\(BZ#1820311\)](#)

### 使用间接 COS 定义时目录服务器不再泄漏内存

在以前的版本中,在处理一个间接 Class Of Service (COS) 定义后, Directory Server 会在每个使用间接 COS 定义的搜索操作中泄漏内存。在这个版本中, Directory 服务器会在处理后释放所有与数据库条目关联的内部 COS 结构。因此,当使用间接 COS 定义时,服务器不会再泄漏内存。

[\(BZ#1816862\)](#)

### 现在添加 AD 用户的 ID 覆盖可以在 IdM Web UI 中正常工作

在以前的版本中,当使用 IdM Web UI 时,为了对管理角色授予访问权限,将活动目录(AD)用户的 ID 覆盖添加到默认信任视图中的身份管理(IdM)组中会失败。在这个版本中,这个程序错误已被解决。现在,在这种情况下,您可以使用 Web UI 和 IdM 命令行界面(CLI)。

[\(BZ#1651577\)](#)

### 在软件包安装过程, FreeRADIUS 不再生成证书

在以前的版本中, FreeRADIUS 会在软件包安装过程中生成证书,这会产生以下问题:

- 如果使用 Kickstart 安装 FreeRADIUS,则可能会在系统中的熵不足时生成证书,从而导致安装失败或者较少的安全证书。
- 很难将软件包构建为镜像的一部分,如容器,因为软件包安装是在构建器机器上而不是目标机器上进行。从镜像生成的所有实例都有相同的证书信息。
- 最终用户很难在其环境中生成一个简单的虚拟机,因为证书必须被删除并手动重新生成。

在这个版本中, FreeRADIUS 安装不再生成默认的自签名 CA 证书,也不会生成从属 CA 证书。当通过 **systemd** 启动 FreeRADIUS 时:

- 如果缺少所有必需的证书,则生成一组默认证书。
- 如果存在一个或多个预期证书,则不会生成新证书。

[\(BZ#1672285\)](#)

### FreeRADIUS 现在生成与 FIPS 兼容的 Diffie-Hellman 参数

由于新的 FIPS 要求不允许 **openssl** 通过 **dhparam** 生成 Diffie-Hellman(dh) 参数,所以从 FreeRADIUS bootstrap 脚本和文件中删除了 dh 参数生成, **RFC3526-group-18-8192.dhparam** 包含在所有系统的 FreeRADIUS 软件包中,从而在 FIPS 模式下启用 FreeRADIUS。

请注意:您可以自定义 **/etc/raddb/certs/bootstrap** 和 **/etc/raddb/certs/Makefile**,以便在需要时恢复 DH 参数生成。

[\(BZ#1859527\)](#)

### 更新 Healthcheck 现在可以正确地更新 ipa-healthcheck-core 和 ipa-healthcheck

在以前的版本中,输入 **yum update healthcheck** 不会更新 **ipa-healthcheck** 软件包,而是使用 **ipa-healthcheck-core** 软件包替换。因此, **ipa-healthcheck** 命令在更新后无法正常工作。

在这个版本中,修正了这个 bug,更新 **ipa-healthcheck** 软件包可以正确地更新 **ipa-healthcheck** 软件包和 **ipa-healthcheck-core** 软件包。因此,在更新后, **Healthcheck** 工具可以正常工作。

[\(BZ#1852244\)](#)

### 5.4.11. 图形基础结构

#### 带有混合 Nvidia GPU 的笔记本电脑现在可以成功恢复挂起

在以前的版本中, **nouveau** 图形驱动程序有时无法在某些笔记本电脑中使用节电模式的混合 Nvidia GPU。因此, 笔记本电脑无法恢复挂起。

在这个版本中,修正了 Runtime Power Management(**runpm**)系统里的几个问题。因此, 带有混合图形的笔记本电脑现在可以成功恢复挂起。

(JIRA:RHELPLAN-57572)

### 5.4.12. 虚拟化

#### 使用默认 CPU 模式迁移虚拟机现在可以更可靠

在以前的版本中, 如果创建虚拟机(VM)时没有指定 CPU 型号,QEMU 会使用 **libvirt** 服务无法看到的默认型号。因此, 可以将虚拟机迁移到不支持虚拟机的默认 CPU 模型的主机上, 这有时会导致迁移后客户端操作系统中的崩溃和错误行为。

在这个版本中, **libvirt** 在虚拟机 XML 配置中明确使用 **qemu64** 模式作为默认型号。因此,如果用户尝试将使用默认 CPU 型号的虚拟机迁移到不支持该型号的主机中, **libvirt** 会正确地生成出错信息。

但请注意, 红帽强烈建议您为虚拟机使用特定的 CPU 型号。

(JIRA:RHELPLAN-45906)

### 5.4.13. 容器

#### 关于 Podman 支持 FIPS 的备注

联邦信息处理标准(FIPS)要求使用经过认证的模块。在以前的版本中, Podman 通过在启动时启用正确的标记, 来在容器中正确地安装经过认证的模块。但是, 在此发行版本中, Podman 没有正确设置系统以 FIPS 系统范围加密形式提供的附加应用程序助手。尽管经过认证的模块不需要设置系统范围的加密策略, 但它确实提高了应用程序以兼容方式使用加密模块的能力。要临时解决这个问题, 请在任何其他应用程序代码被执行前, 更改容器以运行 **update-crypto-policies --set FIPS** 命令。在这个版本中不再需要 **update-crypto-policies --set FIPS** 命令。

(BZ#1804193)

## 5.5. 技术预览

这部分列出了 Red Hat Enterprise Linux 8.3 中的所有技术预览。

如需有关红帽对技术预览功能支持范围的信息, 请参阅 [技术预览功能支持范围](#)。

### 5.5.1. 网络

#### 启用 **xt\_u32** Netfilter 模块

**xt\_u32** Netfilter 模块现在包括在 **kernel-modules-extra** rpm 中。此模块帮助基于不能访问其他基于协议的数据包过滤器的数据进行数据包转发, 从而简化手动迁移到 **nftables**。但是, 红帽不支持 **xt\_u32** Netfilter 模块。

(BZ#1834769)

## nmstate 作为技术预览提供

nmstate 是主机的网络 API。**nmstate** 软件包作为技术预览提供库和 **nmstatectl** 命令行实用程序以声明性方式管理主机网络设置。网络状态由预定义的 schema 描述。报告当前状态以及对所需状态的更改都符合 schema。

详情请查看 [/usr/share/doc/nmstate/README.md](#) 文件以及 [/usr/share/doc/nmstate/examples](#) 目录中的示例。

(BZ#1674456)

## AF\_XDP 作为技术预览

**Address Family eXpress Data Path (AF\_XDP)** 是设计用于处理高性能数据包。它伴随 **XDP**，并将编程选择的数据包的高效重定向授予给用户空间应用程序，以便做进一步处理。

(BZ#1633143)

## XDP 作为技术预览提供

eXpress Data Path (XDP) 功能作为技术预览提供。它提供了在内核入口数据路径早期为高性能数据包处理附加扩展 Berkeley Packet Filter (eBPF) 程序的方法，从而可以进行高效的可编程数据包分析、过滤和操作。

(BZ#1503672)

## KTLS 作为技术预览提供

在 Red Hat Enterprise Linux 8 中，KTLS 是作为技术预览提供的。KTLS 使用内核中的对称加密或者解密算法为 AES-GCM 密码处理 TLS 记录。KTLS 还提供将 TLS 记录加密卸载到支持此功能的网络接口控制器(NIC)的接口。

(BZ#1570255)

## 可作为技术预览的 XDP 功能

红帽提供了以下 eXpress Data Path(XDP)功能作为不受支持的技术预览：

- 在 AMD 和 Intel 64 位以外的构架中载入 XDP 程序。请注意，**libxdp** 库不适用于 AMD 和 Intel 64 位的构架。
- **XDP\_TX** 和 **XDP\_REDIRECT** 返回代码。
- XDP 硬件卸载。在使用这个特性前，请参阅 [在使用 nfp 驱动程序的 Netronome 网卡上卸载 XDP 程序失败](#)。

(BZ#1889737)

## act\_mpls 模块作为技术预览提供

**act\_mpls** 模块现在作为技术预览在 **kernel-modules-extra** rpm 中找到。该模块允许使用流量控制 (TC) 过滤器进行多协议标签交换 (MPLS) 操作，例如：通过 TC 过滤器推送和弹出 MPLS 标签堆栈条目。模块还允许独立设置 Label、Traffic Class、Stack 的 Bottom 和 Time to Live 字段。

(BZ#1839311)

## 多路径 TCP 现在作为技术预览提供

多路径 TCP(MPTCP)现在作为技术预览提供。MPTCP 改进了网络中的资源使用量以及网络故障的恢复能力。例如：在 RHEL 服务器中使用多路径 TCP，启用了 MPTCP v1 的智能手机可以连接到服务器上运行的应用程序，并在 Wi-Fi 和手机网络间切换，而不会中断到服务器的连接。

请注意,在服务器中运行的应用程序必须原生支持 MPTCP 或管理员必须在内核中载入 **eBPF** 程序,以便动态地将 **IPPROTO\_TCP** 改为 **IPPROTO\_MPTCP**。

详情请查看 [多路径 TCP 入门](#)。

(JIRA:RHELPLAN-41549)

### systemd-resolved 服务现在作为技术预览提供

**systemd-resolved** 为本地应用程序提供名字解析。该服务实现了缓存和验证 DNS stub 解析器、链接本地多播名称解析 (LLMNR) 以及多播 DNS 解析器和响应程序。

请注意，即使 **systemd** 软件包提供了 **systemd-resolved**，这个服务也是一个不受支持的技术预览。

(BZ#1906489)

## 5.5.2. 内核

### kexec fast reboot 功能可作为技术预览使用

**kexec fast reboot** 特性仍作为一个技术预览提供。**kexec fast reboot** 通过允许内核直接引导到第二个内核，而无需首先通过基本输入/输出系统(BIOS)，从而显著加快了启动过程。要使用这个功能：

1. 手动加载 **kexec** 内核。
2. 重启操作系统。

(BZ#1769727)

### eBPF 作为技术预览

**Extended Berkeley Packet Filter(eBPF)**是一个内核中的虚拟机,允许在可访问有限功能的受限沙箱环境中在内核空间中执行代码。

虚拟机包含新系统调用 **bpf()**，它支持生成各种映射类型，同时还允许在特殊的装配类代码中载入程序。然后，代码被加载到内核，并使用即时编译方式转换为原生机器代码。请注意,只有具有 **CAP\_SYS\_ADMIN** 能力的用户（如 root 用户）才可以成功使用 **bpf()** syscall。更多信息，请参阅 **bpf(2)** man page。

载入的程序可附加到不同的点（套接字、追踪点、数据包）来接收和处理数据。

红帽提供的很多组件都使用 **eBPF** 虚拟机。每个组件处于不同的开发阶段，因此目前并不完全支持所有组件。所有组件都作为技术预览提供，除非有特定组件被显示为受支持。

以下显著的 **eBPF** 组件当前还作为技术预览提供：

- **bpfftrace** 是使用 **eBPF** 虚拟机的高级别追踪语言。
- **AF\_XDP**，将 **eXpress Data Path (XDP)** 连接到用户空间的套接字，用于优先考虑数据包处理性能的应用程序。

(BZ#1559616)

### igc 驱动程序作为 RHEL 8 的一个技术预览

**igc** Intel 2.5G 以太网 Linux 有线 LAN 驱动程序现在可在 RHEL 8 的所有架构中作为技术预览使用。**ethtool** 还支持 **igc** 有线 LAN。

(BZ#1495358)

### Soft-RoCE 作为一个技术预览提供

通过融合以太网的远程直接内存访问(RDMA)是一个网络协议，其通过以太网实现 RDMA。Soft-RoCE 是 RoCE 的软件实现，它支持两种协议版本，RoCE v1 和 RoCE v2。在 RHEL 8 中，Soft-RoCE 驱动程序 **rdma\_rxe** 作为不受支持的技术预览提供。

(BZ#1605216)

### 5.5.3. 文件系统和存储

#### NVMe/TCP 作为技术预览提供

通过 TCP/IP 网络(NVMe/TCP)访问和共享 Nonvolatile Memory Express(NVMe/TCP)存储及其对应的 **nvme-tcp.ko** 和 **nvmet-tcp.ko** 内核模块已被添加为技术预览。

使用 **nvme-cli** 和 **nvmetcli** 软件包提供的工具可以管理 NVMe/TCP 作为存储客户端或目标。

NVMe/TCP 目标技术预览仅用于测试目的，目前没有计划提供全面支持。

(BZ#1696451)

#### 现在 ext4 和 XFS 作为技术预览提供文件系统 DAX

在 Red Hat Enterprise Linux 8 中，文件系统 DAX 作为技术预览提供。DAX 提供了将持久内存直接映射到其地址空间的方法。要使用 DAX，系统必须有某种可用的持久内存，通常使用一个或多个非线内存模块 (NVDIMM)，且必须在 NVDIMM 上创建支持 DAX 的文件系统。另外，该文件系统必须使用 **dax** 挂载选项挂载。然后，在 **dax** 挂载的文件系统中的一个文件 **mmap** 会把存储直接映射到应用程序的地址空间中。

(BZ#1627455)

#### OverlayFS

OverlayFS 是一种联合文件系统。它允许您在另一个文件系统上覆盖一个文件系统。更改记录在上面的文件系统中，而较小的文件系统则未修改。这允许多个用户共享文件系统镜像，如容器或 DVD-ROM，基础镜像使用只读介质。

在大多数情况下，OverlayFS 仍是一个技术预览。因此，当这个技术被激活时，内核会记录警告信息。

与支持的容器引擎 (**podman**、**cri-o** 或 **buildah**) 一同使用时，对 OverlayFS 提供的全面支持包括以下限制：

- OverlayFS 仅支持作为容器引擎图形驱动程序使用。它只针对容器 COW 内容支持，而不适用于持久性存储。您必须将任何持久性存储放在非 OverlayFS 卷中。您只能使用默认容器引擎配置：一个级别的覆盖、一个较低 **dir** 以及较低级别和上一级都位于同一个文件系统中。
- 目前只支持 XFS 作为较低层文件系统使用。

另外，以下规则和限制适用于使用 OverlayFS:

- OverlayFS 内核 ABI 和用户空间的行为被视为不稳定，将来的更新可能会改变。



- OverlayFS 提供一组受限的 POSIX 标准。在使用 OverlayFS 部署前，先测试您的应用程序。以下情况与 POSIX 不兼容：
  - **O\_RDONLY** 打开的较低文件在读取文件时不会接收 **st\_atime** 更新。
  - 使用 **O\_RDONLY** 打开的较低文件，然后与 **MAP\_SHARED** 映射与后续修改不一致。
  - RHEL 8 中不默认启用完全兼容 **st\_ino** 或 **d\_ino** 值，但您可以使用模块选项或挂载选项为它们启用完整的 POSIX 合规性。  
要获得一致的内节点编号，请使用 **xino=on** 挂载选项。

您还可以使用 **redirect\_dir=on** 和 **index=on** 选项提高 POSIX 合规性。这两个选项使上层的格式与没有这些选项的 overlay 不兼容。也就是说，如果您使用 **redirect\_dir=on** 或 **index=on** 创建一个覆盖，卸载覆盖，然后在没有这些选项的情况下挂载覆盖，则可能会出现意想不到的结果或错误。

- 要确定现有 XFS 文件系统是否有资格用作 overlay，请使用以下命令查看是否启用了 **ftype=1** 选项：

```
# xfs_info /mount-point | grep ftype
```

- 使用 OverlayFS 在所有支持的容器引擎中默认启用 SELinux 安全标签。
- 本发行版本中与 OverlayFS 相关的几个已知问题。详情请查看 Linux 内核文档中的 *非标准行为*：  
<https://www.kernel.org/doc/Documentation/filesystems/overlayfs.txt>。

有关 OverlayFS 的详情请参考 Linux 内核文档：

<https://www.kernel.org/doc/Documentation/filesystems/overlayfs.txt>。

(BZ#1690207)

## Stratis 现在作为技术预览提供

Stratis 是一个新的本地存储管理器。它在存储池的上面为用户提供额外的功能。

Stratis 可让您更轻松地执行存储任务，比如：

- 管理快照和精简配置
- 根据需要自动增大文件系统大小
- 维护文件系统

要管理 Stratis 存储，使用 **stratis** 工具来与 **stratisd** 后台服务进行通信。

Stratis 作为技术预览提供。

如需更多信息，请参阅 Stratis 文档：[设置 Stratis 文件系统](#)。

RHEL 8.3 将 Stratis 更新至 2.1.0 版本。如需更多信息，请参阅 [Stratis 2.1.0 发行注记](#)。

(JIRA:RHELPLAN-1212)

## IdM 现在支持在 IdM 域成员中将 Samba 服务器设置为技术预览

在这个版本中，您可以在 Identity Management(IdM)域成员中设置 Samba 服务器。由同名软件包提供的新 **ipa-client-samba** 程序为 IdM 添加了特定于 Samba 的 Kerberos 服务主体并准备 IdM 客户端。例如，实用程序使用 **sss** ID 映射后端的 ID 映射配置创建 **/etc/samba/smb.conf**。现在，管理员可以在 IdM 域成

员中设置 Samba。

由于 IdM Trust Controller 不支持全局目录服务，AD-enrolled Windows 主机无法在 Windows 中找到 IdM 用户和组。另外，IdM Trust Controller 不支持使用分布式计算环境/远程过程调用(DCE/RPC)协议解析 IdM 组。因此，AD 用户只能访问 IdM 客户端的 Samba 共享和打印机。

详情请查看在 [IdM 域成员中设置 Samba](#)。

(JIRA:RHELPLAN-13195)

#### 5.5.4. 高可用性和集群

##### pcs cluster setup 命令的本地模式版本，可作为技术预览使用

默认情况下，**pcs cluster setup** 命令会自动将所有配置文件与集群节点同步。在 Red Hat Enterprise Linux 8.3 中，**pcs cluster setup** 命令作为技术预览提供 **--corosync-conf** 选项。指定这个选项可将命令切换到本地模式。在这个模式中，**pcs** 会创建一个 **corosync.conf** 文件，并将其只保存到本地节点的指定文件中，而不与其它节点沟通。这可让您在脚本中创建 **corosync.conf** 文件，并使用脚本处理该文件。

([BZ#1839637](#))

##### pacemaker podman bundles 作为技术预览

pacemaker 容器捆绑包现在在 **podman** 容器平台上运行，容器捆绑包功能作为一个技术预览可用。其中一个功能例外于技术预览：红帽完全支持在 Red Hat Openstack 中使用 Pacemaker 捆绑包。

([BZ#1619620](#))

##### 作为技术预览的 corosync-qdevice 中的 Heuristics

Heuristics 是一组在启动、集群成员资格更改、成功连接到 **corosync-qnetd** 时本地执行的命令，以及可选的定期执行的命令。当所有命令及时成功完成（返回的错误代码为零），代表 heuristics 通过，否则代表失败。Heuristics 结果发送到 **corosync-qnetd**，在计算中用来决定哪个分区应该是 quorate。

([BZ#1784200](#))

##### 新的 fence-agents-heuristics-ping 保护代理

作为技术预览，Pacemaker 现在支持 **fence\_heuristics\_ping** 代理。这个代理旨在打开一组实验性保护代理，它们本身没有实际隔离，而是以新的方式利用隔离级别。

如果 heuristics 代理的配置与用于实现实际隔离代理有相同的隔离级别，但在代理之前配置，隔离会在试图进行隔离前，在 heuristics 代理上发出一个 **off** 操作。如果 heuristics 代理给出了 **off** 操作的一个负结果，则代表隔离不成功，从而导致 Pacemaker 隔离跳过对实现隔离的代理发出 **off** 动作的步骤。heuristics 代理可以利用这个行为来防止实际上进行隔离的代理在特定情况下隔离节点。

用户可能希望使用这个代理，特别是在双节点集群中，如果节点可以预先知道无法正确接管该服务，则节点可以隔离这个代理。例如，如果节点在网络连接链接出现问题，使服务无法访问客户端，则节点接管服务可能不真实。在这种情况下，向路由器的 ping 可能会探测到这个情况。

([BZ#1775847](#))

#### 5.5.5. 身份管理

##### 身份管理 JSON-RPC API 作为技术预览

一个 API 可用于 Identity Management(IdM)。要查看 API，IdM 还提供了一个 API 浏览器作为技术预览。

在 Red Hat Enterprise Linux 7.3 中，IdM API 被改进来启用多个 API 命令版本。在以前的版本中，增强功能可能会以不兼容的方式改变命令的行为。用户现在可以继续使用已有的工具和脚本，即使 IdM API 发生了变化。这可启用：

- 管理员要在服务器中使用之前或更高版本的 IdM，而不是在管理客户端中使用。
- 开发人员使用 IdM 调用的特定版本，即使 IdM 版本在服务器上发生了变化。

在所有情况下，与服务器进行通信是可能的，无论是否一方使用，例如，一个新的版本会为这个功能引进新的选项。

有关使用 API 的详细信息，请参阅[使用身份管理 API 与 IdM 服务器通信\(TECHNOLOGY PREVIEW\)](#)。

(BZ#1664719)

### DNSSEC 在 IdM 中作为技术预览提供

带有集成 DNS 的身份管理 (IdM) 服务器现在支持 DNS 安全扩展 (DNSSEC)，这是一组增强 DNS 协议安全性的 DNS 扩展。托管在 IdM 服务器上的 DNS 区可以使用 DNSSEC 自动签名。加密密钥是自动生成和轮转的。

建议那些决定使用 DNSSEC 保护 DNS 区的用户读取并遵循这些文档：

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

请注意，集成了 DNSSEC 的 IdM 服务器验证从其他 DNS 服务器获取的 DNS 答案。这可能会影响未按照推荐的命名方法配置的 DNS 区域可用性。

(BZ#1664718)

## 5.5.6. Desktop

### GNOME 用于 64 位 ARM 架构，作为一个技术预览

GNOME 桌面环境现在可作为技术预览用于 64 位 ARM 架构。这可让管理员使用 VNC 会话从图形用户界面(GUI)远程配置和管理服务器。

因此，在 64 位 ARM 架构中提供了新的管理应用程序。例如：**Disk Usage Analyzer (baobab)**, **防火墙配置 (firewall-config)**, **Red Hat Subscription Manager (subscription-manager)**, 或 **Firefox web 浏览器**。使用 **Firefox**，管理员可以远程地连接到本地 Cockpit 守护进程。

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

### IBM Z 上的 GNOME 桌面作为技术预览提供

GNOME 桌面，包括 Firefox 网页浏览器，现在在 IBM Z 构架中作为技术预览提供。现在，您可以使用 VNC 连接到运行 GNOME 的远程图形会话来配置和管理您的 IBM Z 服务器。

(JIRA:RHELPLAN-27737)

## 5.5.7. 图形基础结构

## VNC 远程控制台作为 64 位 ARM 架构的一个技术预览提供

在 64 位 ARM 架构中,虚拟网络计算(VNC)远程控制台可作为技术预览使用。请注意,在 64 位 ARM 架构中,目前图形堆栈的其它部分没有被验证。

(BZ#1698565)

## Intel Tiger Lake 图形作为技术预览提供

Intel Tiger Lake UP3 和 UP4 Xe 图形现在作为技术预览提供。

要启用 Intel Tiger Lake 图形的硬件加速,请在内核命令行中添加以下选项:

```
i915.force_probe=pci-id
```

在这个选项中,将 *pci-id* 替换为以下之一:

- Intel GPU 的 PCI ID
- 用来启用带有所有 alpha 质量硬件的 **i915** 驱动程序的 \* 字符

(BZ#1783396)

## 5.5.8. Red Hat Enterprise Linux 系统角色

### RHEL 系统角色的 postfix 角色作为技术预览

Red Hat Enterprise Linux 系统角色为 Red Hat Enterprise Linux 子系统提供了一个配置界面,这有助于通过包含 Ansible 角色来简化系统配置。这个界面支持在多个 Red Hat Enterprise Linux 版本间管理系统配置,并使用新的主发行版本。

**rhel-system-roles** 软件包通过 AppStream 软件仓库发布。

**postfix** 角色是作为技术预览提供的。

以下角色被完全支持:

- **kdump**
- **network**
- **selinux**
- **storage**
- **timesync**

如需更多信息,请参阅有关 [RHEL 系统角色的知识库文章](#)。

(BZ#1812552)

## 5.5.9. 虚拟化

### KVM 虚拟化可用于 RHEL 8 Hyper-V 虚拟机

作为技术预览,现在可将嵌套的 KVM 虚拟化用于 Microsoft Hyper-V hypervisor。因此,您可以在运行在 Hyper-V 主机的 RHEL 8 虚拟机中创建虚拟机。

请注意目前，这个功能仅适用于 Intel 系统。另外，在一些情况下，Hyper-V 中不默认启用嵌套虚拟化。要启用它，请参阅以下文档：

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

(BZ#1519039)

## 用于 KVM 虚拟机的 AMD SEV

作为技术预览，RHEL 8 为使用 KVM hypervisor 的 AMD EPYC 主机引入了安全加密虚拟化(SEV)特性。如果在虚拟机(VM)上启用，SEV 会加密虚拟机内存，因此主机不能访问虚拟机上的数据。如果主机被恶意软件成功损坏，这可以提高虚拟机的安全性。

请注意，在单一主机上同时可以使用此功能的虚拟机数量是由主机硬件决定的。当前的 AMD EPYC 处理器支持使用 SEV 运行最多 509 个运行虚拟机。

也请注意，对于将 SEV 配置为可以引导的虚拟机，还必须使用硬内存限制配置虚拟机。要做到这一点，请在虚拟机 XML 配置中添加以下内容：

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

建议 N 的值等于或大于客户机 RAM + 256 MiB。例如：如果为客户端分配 2 GiB RAM，则 N 应该为 2359296 或更高。

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

## Intel vGPU

作为技术预览，现在可以将物理 Intel GPU 设备划分为多个虚拟设备（称为 **mediated devices**）。然后可将这些 mediated devices 分配给多个虚拟机(VM)作为虚拟 GPU。因此,这些虚拟机共享单个物理 Intel GPU 的性能。

请注意,只有所选 Intel GPU 与 vGPU 功能兼容。另外,为虚拟机分配物理 GPU 使得主机无法使用 GPU,并可能阻止主机的图形显示输出工作。

(BZ#1528684)

## 创建嵌套虚拟机

对于在 AMD64 和使用 RHEL 8 的 IBM Z 系统主机上运行的 KVM 虚拟机(VM),嵌套的 KVM 虚拟化是作为技术预览提供的。使用此功能,在物理 RHEL 8 主机上运行的 RHEL 7 或 RHEL 8 虚拟机可作为虚拟机监控程序,并托管自己的虚拟机。

请注意,在 RHEL 8.2 及之后的版本中,在 Intel 64 主机上运行的虚拟机完全支持嵌套虚拟化。

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

## 选择 Intel 网络适配器现在支持 Hyper-V 的 RHEL 客户端中的 SR-IOV

作为技术预览,在 Hyper-V hypervisor 中运行的 Red Hat Enterprise Linux 客户机操作系统现在可以为 **ixgbev** 和 **iavf** 驱动程序支持的 Intel 网络适配器使用单根 I/O 虚拟化(SR-IOV)功能。此功能在满足以下条件时启用：

- 对网络接口控制器(NIC)启用了 SR-IOV 支持
- 对虚拟 NIC 启用了 SR-IOV 支持

- 对虚拟交换机启用 SR-IOV 支持
- NIC 中的虚拟功能(VF)附加到虚拟机

目前，Microsoft Windows Server 2019 和 2016 支持该功能。

(BZ#1348508)

## 5.5.10. 容器

### podman 容器镜像作为技术预览提供

**registry.redhat.io/rhel8/podman** 容器镜像是 **podman** 软件包的一个容器化实施。**podman** 工具用于管理容器和镜像、挂载到这些容器的卷以及从容器组生成的 Pod。Podman 基于 **libpod** 库来管理容器生命周期。**libpod** 库提供用于管理容器、Pod、容器镜像和卷的 API。此容器镜像允许创建、修改并运行容器镜像，而无需在您的系统上安装 **podman** 软件包。使用案例不包括在无根模式下作为非 root 用户运行此镜像。要拉取 **registry.redhat.io/rhel8/podman** 容器镜像，您需要有效的 Red Hat Enterprise Linux 订阅。

(BZ#1627899)

### crun 作为一个技术预览提供

**crun** OCI 运行时被添加到 **container-roots:rhel8** 模块中。**crun** 提供使用 **cgoupsV2** 运行的权限。**crun** 支持一个注解，它允许容器访问无根用户额外组。这对在用户只能访问的目录中或者在该目录中设定目录时很有用。

(BZ#1841438)

### podman-machine 命令不受支持

用于管理虚拟机的 **podman-machine** 命令仅作为技术预览提供。相反，请直接从命令行运行 Podman。

(JIRA:RHELDPCS-16861)

## 5.6. 过时的功能

这部分提供在 Red Hat Enterprise Linux 8 中弃用的功能概述。

弃用的功能可能在以后的主要发行本中不被支持，因此不建议在新的部署中使用。有关特定主要发行本中已弃用功能的最新列表，请参考最新版本的发行业档。

在 Red Hat Enterprise Linux 8 中，已弃用的功能的支持状态保持改变。有关支持长度的详情，请查看 [Red Hat Enterprise Linux 生命周期](#) 和 [Red Hat Enterprise Linux 应用程序流生命周期](#)。

对于当前或将来的主发行版本中的新部署，我们不推荐使用已弃用的硬件组件。硬件驱动程序更新仅限于安全和关键修复。红帽建议尽快替换这个硬件。

一个软件包可以被弃用，我们不推荐在以后使用。在某些情况下，软件包可从产品中删除。然后，产品文档可识别提供类似、完全相同或者更高级功能的最新软件包，并提供进一步建议。

有关 RHEL 7 中存在，但已从 *RHEL 8* 中删除的功能信息，请参阅 [使用 RHEL 8 的注意事项](#)。

### 5.6.1. 安装程序和镜像创建

#### 弃用了一些 Kickstart 命令和选项

使用 RHEL 8 Kickstart 文件中的以下命令和选项会在日志中显示警告信息。

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

如果只列出具体选项，则基础命令及其它选项仍可用且没有弃用。

有关 Kickstart 中的详情和相关更改，请参阅 *使用 RHEL 8 的参考事项* 文档中的 [Kickstart 更改](#) 部分。

(BZ#1642765)

### **ignoredisk Kickstart 命令的 --interactive 选项已被弃用**

在以后的 Red Hat Enterprise Linux 版本中使用 **--interactive** 选项会导致严重安装错误。建议您修改 Kickstart 文件删除该选项。

(BZ#1637872)

### **Image Builder 的 lorax-composer 后端在 RHEL 8 中已弃用**

以前的 Image Builder 的后端 **lorax-composer** 被视为已弃用。它只会为 Red Hat Enterprise Linux 8 生命周期的其余部分获得特定的修复程序，并将在以后的主发行版本中被删除。红帽建议您卸载 **lorax-composer**，改为安装 **osbuild-composer** 后端。

如需了解更多详细信息，请参阅 [生成自定义的 RHEL 系统镜像](#)。

(BZ#1893767)

## **5.6.2. 软件管理**

### **rpmbuild --sign 已弃用**

在这个版本中，**rpmbuild --sign** 命令已过时。在以后的 Red Hat Enterprise Linux 版本中使用这个命令可能会导致错误。建议您使用 **rpmsign** 命令替代。

([BZ#1688849](#))

### 5.6.3. Shell 和命令行工具

#### 对 curl 的 metalink 支持已禁用。

在 curl 功能中发现了一个缺陷，它处理凭证和文件哈希的方式与处理使用 Metalink 下载的内容不匹配。此缺陷允许控制托管服务器的恶意参与者：

- 欺骗用户下载恶意内容
- 在用户不知情的情况下，获得对提供的凭据的未经授权的访问

此漏洞的最大威胁是机密性和完整性。为避免这种情况，在 Red Hat Enterprise Linux 8.2.0.z 中禁用了 curl 的 Metalink 支持。

作为临时解决方案，在下载 Metalink 文件后执行以下命令：

```
wget --trust-server-names --input-metalink`
```

例如：

```
wget --trust-server-names --input-metalink <(curl -s $URL)
```

([BZ#1999620](#))

### 5.6.4. 基础架构服务

#### mailman 已弃用

有了这个更新，**mailman** 软件包已被标记为弃用，并将在以后的 Red Hat Enterprise Linux 主要版本中不提供。

([BZ#1890976](#))

### 5.6.5. 安全性

#### NSS SEED 密码已弃用

Mozilla Network Security Services (**NSS**) 库将不支持在以后的版本中使用 SEED 密码的 TLS 密码组合。为确保在 NSS 取消支持时依赖 SEED 密码的部署平稳过渡，红帽推荐对其它密码套件的支持。

请注意，在 RHEL 中，SEED 密码已经被默认禁用。

([BZ#1817533](#))

#### TLS 1.0 和 TLS 1.1 已弃用

TLS 1.0 和 TLS 1.1 协议在 **DEFAULT** 系统范围的加密策略级别被禁用。如果需要使用启用的协议，如 Firefox 网页浏览器中的视频检查程序，把系统范围的加密策略切换到 **LEGACY** 级别：

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

如需更多信息，请参阅红帽客户门户网站中的知识库文章 [RHEL 8 中的强加密默认值和弱加密算法的弃用](#) 和 [update-crypto-policies\(8\)](#) 手册页。



[\(BZ#1660839\)](#)

## 在 RHEL 8 中弃用 DSA

数字签名算法(DSA)在 Red Hat Enterprise Linux 8 中被视为已弃用。依赖于 DSA 密钥的身份验证机制在默认配置中不起作用。请注意，即使使用系统范围的 **LEGACY** 加密策略级别中，**OpenSSH** 客户端都不接受 DSA 主机密钥。

[\(BZ#1646541\)](#)

## SSL2 Client Hello 在 NSS 中已弃用

传输层安全性(TLS)协议版本 1.2 和更早版本允许以与安全套接字层(SSL)协议版本 2 向后兼容方式与 **Client Hello** 消息开始协商。网络安全服务(NSS)库中对这个功能的支持已被弃用，默认是禁用的。

需要这个功能支持的应用程序需要使用新的 **SSL\_ENABLE\_V2\_COMPATIBLE\_HELLO** API 启用它。以后的 Red Hat Enterprise Linux 8 版本中可以完全删除对这个功能的支持。

[\(BZ#1645153\)](#)

## TPM 1.2 已被弃用

Trusted Platform Module (TPM) 安全加密处理器标准版本在 2016 年更新至 2.0 版本。TPM 2.0 比 TPM 1.2 提供了很多改进，它和之前的版本不向后兼容。在 RHEL 8 中弃用了 TPM 1.2，它可能会在下一个主发行版本中删除。

[\(BZ#1657927\)](#)

## 5.6.6. 网络

### 在 RHEL 8 中已弃用网络脚本

网络脚本在 Red Hat Enterprise Linux 8 中已弃用，且不再默认提供。基本安装提供了 **ifup** 和 **ifdown** 脚本的新版本，它们通过 **nmcli** 工具调用 **NetworkManager** 服务。在 Red Hat Enterprise Linux 8 中，要运行 **ifup** 和 **ifdown** 脚本，**NetworkManager** 必须正在运行。

请注意，**/sbin/ifup-local**、**ifdown-pre-local** 和 **ifdown-local** 脚本中的自定义命令不会执行。

如果需要这些脚本，您仍可以使用以下命令在系统中安装已弃用的网络脚本：

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

**ifup** 和 **ifdown** 脚本链接到已安装的旧网络脚本。

调用旧的网络脚本会显示一个关于它们已过时的警告。

[\(BZ#1647725\)](#)

## 5.6.7. 内核

### 使用无磁盘引导为 Real Time 8 安装 RHEL 现已弃用

无磁盘引导允许多个系统通过网络共享一个 root 文件系统。无盘引导是方便的，它在实时工作负载中容易引入网络延迟。在以后的 RHEL for Real Time 8 的更新中，无盘引导功能将不再被支持。

[\(BZ#1748980\)](#)

### qla3xxx 驱动程序已弃用

在 RHEL 8 中已弃用 **qla3xxx** 驱动程序。本产品的将来主发行版本可能不支持该驱动程序，因此不建议在新的部署中使用该驱动程序。

(BZ#1658840)

### dl2k、dnet、ethoc 和 dlci 驱动程序已弃用

在 RHEL 8 中弃用了 **dl2k**、**dnet**、**ethoc** 和 **dlci** 驱动程序。在以后的主要发行本中，这些驱动程序可能不被支持，因此不建议在新的部署中使用这些驱动程序。

(BZ#1660627)

### rdma\_rxe Soft-RoCE 驱动程序已弃用

通过融合以太网(Soft-RoCE)的软件远程直接内存（也称为 RXE）是模拟远程直接内存访问(RDMA)的一个特性。在 RHEL 8 中，Soft-RoCE 特性作为一个不受支持的技术预览提供。但是，由于稳定性问题，此特性已被弃用，并将在 RHEL 9 中删除。

(BZ#1878207)

## 5.6.8. 文件系统和存储

### elevator 内核命令行参数已弃用

在之前的 RHEL 版本中使用 **elevator** 内核命令行参数为所有设备设置磁盘调度程序。在 RHEL 8 中，该参数已弃用。

上游 Linux 内核删除了对 **elevator** 参数的支持，但出于兼容性的原因，在 RHEL 8 中仍提供此支持。

请注意，内核会根据设备类型选择默认磁盘调度程序。这通常是最佳设置。如果您需要不同的调度程序，红帽建议您使用 **udev** 规则或 Tuned 服务来配置它。匹配所选设备并只为那些设备切换调度程序。

如需更多信息，请参阅[设置磁盘调度程序](#)。

(BZ#1665295)

### LVM mirror 已弃用

LVM **mirror** segment 类型已弃用。以后的 RHEL 主发行版本中会删除对 **mirror** 的支持。

红帽建议使用 segment 类型为 **raid1** 的 LVM RAID 1 设备来替代 **mirror**。**raid1** segment 类型是默认的 RAID 配置类型，它作为推荐的解决方案替换 **mirror**。

要将 **mirror** 设备转换为 **raid1**，请参阅[将镜像 LVM 设备转换为 RAID1 逻辑卷](#)。

LVM **mirror** 有几个已知问题。详情请查看[文件系统和存储中的已知问题](#)。

(BZ#1827628)

### peripety 已被弃用

从 RHEL 8.3 开始，**pipety** 软件包已弃用。

Peripety 存储事件通知守护进程将系统存储日志解析为结构化的存储事件。它帮助您调查存储问题。

(BZ#1871953)

## 禁用了 NFSv3 over UDP

默认情况下，NFS 服务器不再默认在 User Datagram Protocol(UDP)套接字上打开或监听。这个变化只影响 NFS 版本 3，因为版本 4 需要传输控制协议(TCP)。

RHEL 8 不再支持通过 UDP 的 NFS。

(BZ#1592011)

## cramfs 已被弃用

由于缺少用户，**cramfs** 内核模块已被弃用。建议将 **squashfs** 作为一个替代解决方案。

(BZ#1794513)

## 5.6.9. 身份管理

### openssh-ldap 已被弃用

在 Red Hat Enterprise Linux 8 中弃用 **openssh-ldap** 子软件包，并将在 RHEL 9 中删除。因为 **openssh-ldap** 子软件包没有被上游维护，红帽建议您使用 SSSD 和 **sss\_ssh\_authorizedkeys** 帮助程序，它们与其他 IdM 解决方案更好地集成且更安全。

默认情况下，SSSD **ldap** 和 **ipa** 供应商会读取用户对象的 **sshPublicKey** LDAP 属性（如果可用）。请注意，您无法为 **ad** provider 或 IdM 可信域使用默认的 SSSD 配置从 Active Directory(AD)检索 SSH 公钥，因为 AD 没有存储公钥的默认 LDAP 属性。

要允许 **sss\_ssh\_authorizedkeys** 帮助程序从 SSSD 获取密钥，在 **sssd.conf** 文件的 **services** 选项中添加 **ssh** 来启用 **ssh** 响应程序。详情请查看 **sssd.conf(5)** 手册页。

要允许 **sshd** 使用 **sss\_ssh\_authorizedkeys**，添加 **AuthorizedKeysCommand/usr/bin/sss\_ssh\_authorizedkeys** 和 **AuthorizedKeysCommandUser nobody** 选项到 **/etc/ssh/sshd\_config** 文件，如 **ss\_ssh\_authorizedkeys(1)** 手册页所述。

(BZ#1871025)

### 已经删除了 DES 和 3DES 加密类型

由于安全考虑，自 RHEL 7 开始，数据加密标准(DES)算法已被弃用并默认禁用。通过最近重新构建 Kerberos 软件包，已从 RHEL 8 中删除了 single-DES(DES)和 triple-DES (3DES) 加密类型。

如果您已经将服务或用户配置为只使用 DES 或 3DES 加密，您可能会遇到服务中断，例如：

- Kerberos authentication 错误
- **unknown enctype** 加密错误
- 带有 DES 加密数据库主密钥(**K/M**)的 KDC 无法启动

执行以下操作准备升级：

1. 检查您的 KDC 是否使用 DES 或者 3DES 加密，并使用 **krb5check** 打开源 Python 脚本。请参阅 GitHub 上的 [krb5check](#)。
2. 如果您要将 DES 或 3DES 加密用于任何 Kerberos 主体，请使用支持的加密类型重新加密，比如高级加密标准(AES)。有关重新打包的步骤，请参考 MIT Kerberos 文档中的 [Retiring DES](#)。
3. 通过在升级前临时设置以下 Kerberos 选项，从 DES 和 3DES 测试测试：

- a. 在 KDC 上的 `/var/kerberos/krb5kdc/kdc.conf` 中设置 `support_encytypes` 且不包含 `des` 或 `des3`。
  - b. 对于每个主机，在 `/etc/krb5.conf` 以及 `/etc/krb5.conf.d` 中的任意文件，将 `allow_weak_crypto` 设为 `false`。默认为 `false`。
  - c. 对于每个主机，在 `/etc/krb5.conf` 以及 `/etc/krb5.conf.d` 中的任意文件设置 `allowed_encytypes`, `default_tgs_encytypes`, 以及 `default_tkt_encytypes` 且不包含 `des` 或 `des3`。
4. 如果您没有遇到上一步中测试 Kerberos 设置的服务中断，请删除并升级它们。升级到最新的 Kerberos 软件包后您不需要这些设置。

(BZ#1877991)

### SMB1 协议在 Samba 中被弃用

从 Samba 4.11 开始，不安全的服务器消息块版本 1 (SMB1) 协议已弃用，并将在以后的发行版本中删除。

为提高安全性，在 Samba 服务器和客户端工具中默认禁用 SMB1。

(JIRA:RHELDPCS-16612)

## 5.6.10. Desktop

### libgnome-keyring 库已弃用

`libgnome-keyring` 库已弃用，现在使用 `libsecret` 库，因为 `libgnome-keyring` 没有被上游维护，且不会遵循 RHEL 所需的加密策略。新的 `libsecret` 库是符合所需安全标准的替换。

(BZ#1607766)

### AlternateTab 扩展已被删除

提供 AlternateTab GNOME Shell 扩展的 `gnome-shell-extension-alternate-tab` 软件包已被删除。

要配置窗口切换行为，请在键盘设置中设置一个键盘快捷方式。如需更多信息，请参阅以下文章：[在 Gnome 3.32 或更高版本中使用 Alternate-Tab](#)。(BZ#1922488)

## 5.6.11. 图形基础结构

### 不再支持 AGP 图形卡

Red Hat Enterprise Linux 8 不支持使用图形端口 (AGP) 总线的图形卡。推荐使用 PCI-Express bus 图形卡替换。

(BZ#1569610)

## 5.6.12. Web 控制台

### Web 控制台不再支持不完整翻译

RHEL web 控制台不再提供翻译少于 50% 的语言支持。如果浏览器要求转换成这种语言，用户界面将为英语。

(BZ#1666722)

### 5.6.13. Red Hat Enterprise Linux 系统角色

#### geoipupdate 软件包已弃用

**geoipupdate** 软件包需要第三方订阅，同时下载专有内容。因此，**geoipupdate** 软件包已被弃用，并将在下一个主要 RHEL 版本中删除。

(BZ#1874892)

### 5.6.14. 虚拟化

#### virt-manager 已被弃用

虚拟机管理器（也称 **virt-manager**）已弃用。RHEL 8 web 控制台（也称 **Cockpit**）旨在在以后的版本中成为它替换。因此，建议您使用 web 控制台使用 GUI 管理虚拟化。但请注意，**virt-manager** 中的一些功能可能还不能使用 RHEL 8 web 控制台。

(JIRA:RHELPLAN-10304)

#### RHEL 8 不支持虚拟机快照

当前创建虚拟机(VM)快照的机制已经被弃用，因为它无法可靠工作。因此，建议在 RHEL 8 中使用虚拟机快照。

请注意，一个新的 VM 快照机制正在开发中，并将在以后的 RHEL 8 次要发行本中完全实现。

(BZ#1686057)

#### Cirrus VGA 虚拟 GPU 类型已弃用

随着 Red Hat Enterprise Linux 的主要更新，**Cirrus VGA** GPU 设备将在 KVM 虚拟机中不再被支持。因此，红帽建议您使用 **stdvga**、**virtio-vga** 或者 **qxl** 设备而不是 Cirrus VGA。

(BZ#1651994)

#### SPICE 已被弃用

在 RHEL 8.3 中，SPICE 远程显示协议已弃用。请注意，RHEL 8 中仍支持 SPICE，但红帽建议您为远程显示流使用备选解决方案：

- 要访问远程控制台，请使用 VNC 协议。
- 对于高级远程显示功能，请使用 RDP、HP RGS 或 Mechdyne TGX 等第三方工具。

(BZ#1849563)

### 5.6.15. 容器

#### 基于 podman varlink 的 REST API V1 已被弃用

基于 Podman varlink 的 REST API V1 已被上游弃用，以新的 Podman REST API V2 替代。这个功能将在以后的 Red Hat Enterprise Linux 8 发行版本中删除。

(JIRA:RHELPLAN-60226)

### 5.6.16. 已弃用的软件包

下列软件包已弃用，可能不会包括在 Red Hat Enterprise Linux 未来的主发行版本中：

- 389-ds-base-legacy-tools
- authd
- custodia
- hostname
- libidn
- lorax-composer
- mercurial
- net-tools
- network-scripts
- nss-pam-ldapd
- sendmail
- yp-tools
- ypbind
- ypserv

## 5.7. 已知问题

这部分论述了 Red Hat Enterprise Linux 8.3 中已知的问题。

### 5.7.1. 安装程序和镜像创建

#### **auth 和 authconfig Kickstart 命令需要 AppStream 软件仓库**

**auth** 和 **authconfig** Kickstart 命令在安装过程中需要 **authselect-compat** 软件包。如果没有这个软件包，如果使用了 **auth** 或 **authconfig**，则安装会失败。但根据设计，**authselect-compat** 软件包只包括在 AppStream 仓库中。

要临时解决这个问题，请确定安装程序可使用 BaseOS 和 AppStream 软件仓库，或者在安装过程中使用 **authselect** Kickstart 命令。

(BZ#1640697)

#### **reboot --kexec 和 inst.kexec 命令不提供可预测的系统状态**

使用 **reboot --kexec** Kickstart 命令或 **inst.kexec** 内核引导参数执行 RHEL 安装不会提供与完全重启相同的可预期系统状态。因此，在不重启的情况下切换安装的系统可能会导致无法预计的结果。

请注意，**kexec** 功能已弃用，并将在以后的 Red Hat Enterprise Linux 版本中删除。

(BZ#1697896)

#### **在安装程序中不默认启用网络访问**

几个安装功能需要网络访问，例如：使用 Content Delivery Network(CDN)、NTP 服务器支持和网络安装源注册系统。但默认情况下不启用网络访问，因此在启用网络访问前无法使用这些功能。

要临时解决这个问题，请添加 `ip=dhcp` 在启动安装时启用网络访问。另外，使用引导选项传递 Kickstart 文件或位于网络中的库也会解决这个问题。因此可以使用基于网络的安装功能。

(BZ#1757877)

### 新的 `osbuild-composer` 后端不会在升级时从 `lorax-composer` 复制蓝图状态

对于从 `lorax-composer` 后端升级到新 `osbuild-composer` 后端的 Image Builder 用户，蓝图可能会消失。因此，升级完成后，蓝图不会自动显示。要临时解决这个问题，请执行以下步骤。

#### 先决条件

- `composer-cli` CLI 工具已安装。

#### 流程

1. 运行该命令，将之前基于 `lorax-composer` 的蓝图加载到新 `osbuild-composer` 后端：

```
$ for blueprint in $(find /var/lib/lorax/composer/blueprints/git/workspace/master -name
*.toml); do composer-cli blueprints push "${blueprint}"; done
```

因此，相同的蓝图现在可在 `osbuild-composer` 后端提供。

#### 其它资源

- 有关此已知问题的详情，请参阅[镜像构建器蓝图在 Red Hat Enterprise Linux 8.3 的更新后不再存在](#)。

(BZ#1897383)

### Kickstart 安装无法使用自签名 HTTPS 服务器

目前，当在 kickstart 文件中指定安装源并使用 `--noverifyssl` 选项时，安装程序无法从自签名的 https 服务器安装：

```
url --url=https://SERVER/PATH --noverifyssl
```

要临时解决这个问题，请在开始 kickstart 安装时将 `inst.noverifyssl` 参数附加到内核命令行中。

例如：

```
inst.ks=<URL> inst.noverifyssl
```

(BZ#1745064)

### 如果在仓库刷新完成前尝试使用 CDN 取消注册，则 GUI 安装可能会失败

从 RHEL 8.2 开始，当使用 Content Delivery Network(CDN)注册您的系统并附加订阅时，GUI 安装程序会启动对仓库元数据的刷新。刷新过程不是注册和订阅过程的一部分，因此在 **Connect to Red Hat** 窗口中启用了 **Unregister** 按钮。根据网络连接，刷新过程可能需要一分钟以上的时间完成。如果您在刷新过程完成前点 **Unregister** 按钮，则 GUI 安装可能会失败，因为未注册过程会删除 CDN 仓库文件和安装程序与 CDN 通信所需的证书。

要临时解决这个问题，点 **连接到红帽** 窗口中的 **Register** 按钮后在 GUI 安装中完成以下步骤：

1. 在 **连接到红帽** 窗口中点 **完成** 返回 **安装概述** 窗口。
2. 在 **安装概述** 窗口中验证 **安装源** 和 **软件选择状态** 信息是否以斜体显示任何处理信息。
3. 当安装源和软件选择类别准备好后，点 **连接到红帽**。
4. 点 **Unregister** 按钮。

执行这些步骤后，您可以在 GUI 安装过程中安全地取消注册系统。

(BZ#1821192)

### 属于多个机构的用户帐户注册失败

目前，当试图使用属于多个机构的用户帐户注册系统时，注册过程会失败并显示出错信息，**You must specify an organization for new units**。

要临时解决这个问题，您可以：

- 使用不属于多个机构的不同用户帐户。
- 使用 GUI 和 Kickstart 安装的的 **Connect to Red Hat** 中的 **Activation Key** 验证方法。
- 跳过连接到红帽的注册步骤，并使用 **Subscription Manager** 在安装后注册您的系统。

(BZ#1822880)

### 当使用安装程序引导选项配置 InfiniBand 网络接口时，RHEL 安装程序无法启动

当您使用安装程序引导选项（例如：使用 PXE 服务器下载安装程序镜像）在 RHEL 安装的早期配置 InfiniBand 网络接口时，安装程序无法激活网络接口。

这是因为 RHEL NetworkManager 无法识别 InfiniBand 模式中的网络接口，而是为接口配置以太网连接。

因此，连接激活会失败，且在早期需要 InfiniBand 界面的连接，RHEL 安装程序无法启动安装。

要解决这个问题，使用 **Lorax** 工具创建一个包括更新的 **Anaconda** 和 **NetworkManager** 软件包的新安装介质。

有关创建新安装介质（包括更新的 **Anaconda** 和 **NetworkManager** 软件包，使用 **Lorax** 工具）的详情，请参考[使用 InfiniBand 网络接口安装 Red Hat Enterprise Linux 8.3.0](#)。

(BZ#1890261)

### 当 NVDIMM 设备命名空间设为 devdax 模式时，Anaconda 安装会失败。

在 GUI 安装前，**Anaconda** 安装在 NVDIMM 设备命名空间设为 **devdax** 模式引导后会失败，并带有 **trackback** 信息。

要临时解决这个问题，请在安装开始前重新配置 NVDIMM 设备，将命名空间设置为与 **devdax** 模式不同的模式。因此，您可以继续安装。

(BZ#1891827)

### 当使用使用第三方工具创建的 USB 引导安装时，不会检测本地介质安装源



当从使用第三方工具创建的 USB 引导 RHEL 安装时，安装程序无法检测 **本地介质** 安装源（只检测 '红帽 CDN'）。

造成此问题的原因是默认引导选项 `inst.stage2=` 尝试搜索 `iso9660` 镜像格式。但是，第三方工具可能会创建具有不同格式的 ISO 镜像。

作为临时解决方案，请使用以下解决方案之一：

- 当引导安装时，点击 **Tab** 键来编辑内核命令行，并将引导选项 `inst.stage2=` 改为 `inst.repo=`。
- 要在 Windows 中创建可引导 USB 设备，使用 Fedora Media Writer。
- 使用 Rufus 等第三方工具创建可引导 USB 设备时，首先在 Linux 系统上重新生成 RHEL ISO 镜像，然后使用第三方工具创建可引导 USB 设备。

有关执行任何指定临时解决方案的步骤的更多信息，请参阅[安装 RHEL 8.3 过程中不会自动探测到安装介质](#)

(BZ#1877697)

### Anaconda 现在在文本模式中显示 `lidl` 或未格式化的 DASD 磁盘对话框

在以前的版本中，在文本模式的安装过程中，Anaconda 无法显示 Linux 磁盘布局(`lidl`)或未格式化的直接访问存储设备(DASD)磁盘的对话框。因此，用户无法将这些磁盘用于安装。

有了这个更新，在文本模式中，Anaconda 会识别 `lidl` 和未格式化的 DASD 磁盘，并显示一个对话框，其中用户可以正确格式化它们以备将来安装使用。

(BZ#1874394)

### 使用图形安装程序时，Red Hat Insights 客户端无法注册操作系统

目前，安装会失败，并显示结尾时指向 Insights 客户端的错误。

要临时解决这个问题，在安装程序注册系统前，在 **连接到 Red Hat** 这一步骤取消选择 **Connect to Red Hat Insights** 选项。

因此，您可以使用以下命令完成安装并在以后注册到 Insights：

```
# insights-client --register
```

(BZ#1931069)

## 5.7.2. 订阅管理

`syspurpose addons` 对 `subscription-manager attach --auto` 输出没有影响。

在 Red Hat Enterprise Linux 8 中，添加了 `syspurpose` 命令行工具的四个属性：`role`、`usage`、`service_level_agreement` 和 `addons`。目前，只有 `role`、`usage` 和 `service_level_agreement` 会影响到运行 `subscription-manager attach --auto` 命令的输出。试图为 `addons` 参数设置值的用户不会观察到对自动附加的订阅有任何影响。

(BZ#1687900)

## 5.7.3. 基础架构服务

运行 `dnf update` 时会删除 `libmaxminddb-devel-debuginfo.rpm`

当执行 `dnf update` 命令时，二进制 `mmdblookup` 工具会从 `libmaxminddb-devel` 子软件包移到主 `libmaxminddb` 软件包中。因此，`libmaxminddb-devel-debuginfo.rpm` 被删除，这可能会为这个软件包创建错误的更新路径。要临时解决这个问题，请在执行 `dnf update` 命令前删除 `libmaxminddb-devel-debuginfo`。

注意：`libmaxminddb-debuginfo` 是新的 `debuginfo` 软件包。

(BZ#1642001)

## 5.7.4. 安全性

### 锁定的用户可以运行 `sudo`

在使用 **ALL** 关键字定义的 `sudoers` 权限的系统中，拥有权限的 `sudo` 用户可以以帐户被锁定的用户的身份运行 `sudo` 命令。因此，仍然可以使用锁定的和过期的帐号来执行命令。

要临时解决这个问题，请启用新实现的 `runas_check_shell` 选项，并在 `/etc/shells` 中正确设置有效 shell。这样可防止攻击者在比如 `bin` 的系统帐户中运行命令。

(BZ#1786990)

### gnutls 无法恢复使用 NSS 服务器的当前会话

当恢复 TLS（传输层安全）1.3 会话时，**GnuTLS** 客户端会等待 60 毫秒，加上服务器发送会话恢复数据的预计往返时间。如果服务器没有在此时间内发送恢复数据，客户端会创建一个新的会话，而不是恢复当前会话。这不会造成严重的负面影响，只会对常规会话协商的性能有小的影响。

(BZ#1677754)

### libselinux-python 只能通过其模块提供

`libselinux-python` 软件包只包含用于开发 SELinux 应用程序的 Python 2 绑定，它用于向后兼容。因此，通过 `dnf install libselinux-python` 命令，默认的 RHEL 8 软件仓库不再提供 `libselinux-python`。

要临时解决这个问题，请启用 `libselinux-python` 和 `python27` 模块，并使用以下命令安装 `libselinux-python` 软件包及其相依性软件包：

```
# dnf module enable libselinux-python
# dnf install libselinux-python
```

或者，使用它的安装配置集在一个命令中安装 `libselinux-python`：

```
# dnf module install libselinux-python:2.8/common
```

因此，您可以使用相关的模块安装 `libselinux-python`。

(BZ#1666328)

### UDICA 仅在使用 `--env container=podman` 启动时才会处理 UBI 8 容器

Red Hat Universal Base Image 8 (UBI 8) 容器将 `container` 环境变量设置为 `oci` 值，而不是 `podman` 值。这可以防止 `udica` 工具分析容器 JavaScript 对象表示法 (JSON) 文件。

要临时解决这个问题，请使用带有 `--env container=podman` 参数的 `podman` 命令启动 UBI 8 容器。因此，只有当使用上述的临时解决方案时，`udica` 才可以为 UBI 8 容器生成一个 SELinux 策略。

(BZ#1763210)

## 默认日志设置在性能上的负面影响

默认日志环境设置可能会消耗 4 GB 内存甚至更多，当 **systemd-journald** 使用 **rsyslog** 运行时，速率限制值的调整会很复杂。

如需更多信息，请参阅 [RHEL 默认日志设置对性能的负面影响及环境方案](#)。

(JIRA:RHELPLAN-10431)

## /etc/passwd- 的文件权限与 CIS RHEL 8 基准 1.0.0 不一致

由于 CIS Benchmark 存在问题，修正 SCAP 规则可以确保 **/etc/passwd-** backup 文件中的权限被配置为 **0644**。但是 **CIS Red Hat Enterprise Linux 8 Benchmark 1.0.0** 需要该文件的文件权限 **0600**。因此，在修复后，**/etc/passwd-** 的文件权限与基准数据不一致。

(BZ#1858866)

## /etc/selinux/config 中的 SELINUX=disabled 无法正常工作

在 **/etc/selinux/config** 中使用 **SELINUX=disabled** 选项禁用 SELinux 会导致一个进程，在这个进程中，内核启动时启用了 SELinux，并在稍后的启动过程中切换到禁用模式。这可能导致内存泄漏。

要临时解决这个问题，请在内核命令行中添加 **selinux=0** 参数来禁用 SELinux，如 [使用 SELinux 中的在引导时更改 SELinux 模式](#) 部分所述。

(JIRA:RHELPLAN-34199)

## ssh-keyscan 无法在 FIPS 模式中检索服务器的 RSA 密钥

在 FIPS 模式中的 RSA 签名禁用了 **SHA-1** 算法，这样可防止 **ssh-keyscan** 工具程序获取在那个模式下运行的服务器的 RSA 密钥。

要临时解决这个问题，使用 ECDSA 密钥，或者使用服务器中的 **/etc/ssh/ssh\_host\_rsa\_key.pub** 文件在本地检索密钥。

(BZ#1744108)

## OpenSSL 错误处理 PKCS #11 tokens 不支持原始 RSA 或 RSA-PSS 签名

**OpenSSL** 库不会检测到 PKCS #11 令牌的与键相关的功能。因此，当使用不支持原始 RSA 或 RSA-PSS 签名的令牌创建签名时，建立 TLS 连接会失败。

要临时解决这个问题，请在 **/etc/pki/tls/openssl.cnf** 文件的 **crypto\_policy** 部分的 **.include** 行后面添加以下行：

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

因此，可以在描述的场景中建立 TLS 连接。

(BZ#1685470)

## FIPS 模式中的 openssl 只接受特定的 D-H 参数

在 FIPS 模式中，使用 OpenSSL 的传输安全性层(TLS)客户端返回一个 **bad dh value** 错误，并在使用手动生成的参数的服务器中保存 TLS 连接。这是因为 OpenSSL 当配置为符合 FIPS 140-2 时，只可用于符合 NIST SP 800-56A rev3 附件 D (RFC 3526 中定义的组 14、15、16、17 和 18,以及 RFC 7919) 中定义

的组。另，使用 OpenSSL 的服务器会忽略所有其他参数，并选择类似大小的已知参数。要临时解决这个问题，请只使用兼容的组。

(BZ#1810911)

### 删除 rpm-plugin-selinux 软件包会导致从系统中删除所有 selinux-policy 软件包

删除 **rpm-plugin-selinux** 软件包会禁用机器中的 SELinux。它还会从系统中删除所有 **selinux-policy** 软件包。重复安装 **rpm-plugin-selinux** 软件包后会安装 **selinux-policy-minimum** SELinux 策略，即使之前系统中存在 **selinux-policy-targeted** 策略。但是，重复安装不会更新 SELinux 配置文件来考虑策略的改变。因此，即使重新安装 **rpm-plugin-selinux** 软件包也会禁用 SELinux。

要临时解决这个问题：

1. 输入 `umount /sys/fs/selinux/` 命令。
2. 手动安装缺少的 **selinux-policy-targeted** 软件包。
3. 编辑 `/etc/selinux/config` 文件以便策略等同于 **SELINUX=enforcing**。
4. 输入命令 `load_policy -i`。

因此，SELinux 被启用并运行和以前相同的策略。

(BZ#1641631)

### systemd 服务无法从任意路径执行命令

**systemd** 服务无法从 `/home/user/bin` 任意路径执行命令，因为 SELinux 策略软件包不包括任何这样的规则。因此，在非系统路径中执行的自定义服务会失败，并最终会在 SELinux 拒绝访问时记录 Access Vector Cache(AVC)拒绝审核信息。要临时解决这个问题，请执行以下操作之一：

- 使用带有 `-c` 选项的 shell 脚本执行该命令。例如：

```
bash -c command
```

- 从常用的命令路径 `/bin`、`/sbin`、`/usr/sbin`、`/usr/local/bin` 和 `/usr/local/sbin` 中执行命令。

(BZ#1860443)

### rpm\_verify\_permissions 在 CIS 配置集中失败

**rpm\_verify\_permissions** 规则将文件权限与软件包默认权限进行比较。但是，由 **scap-security-guide** 软件包提供的互联网安全中心(CIS)配置将某些文件权限更改为比默认权限更严格。因此，使用 **rpm\_verify\_permissions** 验证某些文件会失败。

要临时解决这个问题，请手动验证这些文件是否具有以下权限：

- `/etc/cron.d` (0700)
- `/etc/cron.hourly` (0700)
- `/etc/cron.monthly` (0700)
- `/etc/crontab` (0600)
- `/etc/cron.weekly` (0700)

- `/etc/cron.daily` (0700)

(BZ#1843913)

### Kickstart 在 RHEL 8 中使用 `org_fedora_oscaps` 而不是 `com_redhat_oscaps`

Kickstart 引用开放安全内容自动化协议(OSCAP)Anaconda 附加组件作为 `org_fedora_oscaps`，而不是 `com_redhat_oscaps`，这可能会导致混淆。这样做可以保持与 Red Hat Enterprise Linux 7 的向后兼容性。

(BZ#1665082)

### 某些 SSG 中的规则组可能会失败

由于未定义规则及其依赖项的顺序，基准中 **SCAP 安全指南**(SSG)规则的修复可能会失败。如果需要以特定顺序执行两个或多个规则，例如，当一条规则安装组件和另一个规则配置同一组件时，它们可按错误的顺序运行，并报告错误。要临时解决这个问题，请执行补救两次，第二次运行会修复依赖规则。

(BZ#1750755)

### OSCAP Anaconda Addon 不会在文本模式中安装所有软件包

如果安装运行在文本模式下，则 **OSCAP Anaconda Addon** 插件无法修改系统安装程序为安装所选择的软件包列表。因此，当使用 Kickstart 指定安全策略配置集且安装以文本模式运行时，安全策略所需的附加软件包不会在安装过程中安装。

要临时解决这个问题，可以使用图形模式运行安装，或者在 Kickstart 文件的 `%packages` 部分指定安全策略配置集所需的所有软件包。

因此，在没有描述的一个临时解决方案的情况下，安全策略配置集所需的软件包不会在 RHEL 安装过程中安装，且安装的系统与给定的安全策略配置集不兼容。

(BZ#1674001)

### OSCAP Anaconda Addon 组件无法正确处理自定义配置集

**OSCAP Anaconda Addon** 插件无法以独立文件中自定义的方式正确处理安全配置集。因此，即使您在对应的 Kickstart 部分正确指定了自定义配置集，RHEL 图形安装中也不会提供自定义配置集。

要临时解决这个问题，请遵循 [从原始 DS 创建单一 SCAP 数据流中的说明,以及一个定制文件](#) 知识库文章。因此，您可以在 RHEL 图形安装中使用自定义的 SCAP 配置集。

(BZ#1691305)

### 基于 OSPP 的配置集与 GUI 软件包组不兼容。

服务器安装的 GUI 软件包组的 **GNOME** 软件包需要 `nfs-utils` 软件包，该软件包与操作系统保护配置集(OSPP)不兼容。因此，在安装带有基于 OSPP 或 OSPP 配置文件（例如安全技术实现指南(STIG)的系统的过程中，选择 *Server with GUI* 软件包组，OpenSCAP 会显示一条警告信息，表示所选的软件包组与安全策略不兼容。如果在安装后应用了基于 OSPP 的配置集，则系统将无法引导。要临时解决这个问题,请不要在使用 OSPP 配置集和基于 OSPP 的配置集时使用 *Server with GUI* 或者其它安装 GUI 的组。在使用 *Server* 或 *Minimal Install* 软件包组时，系统不会有任何问题并可正常工作。

(BZ#1787156)

### 无法使用 *Server with GUI* 或 *Workstation* 软件选择和 CIS 安全配置集进行安装

CIS 安全配置集与 **Server with GUI** 和 **Workstation** 不兼容。因此，无法使用 **Server with GUI** 软件选择和 CIS 配置集进行 RHEL 8 安装。使用 CIS 配置集进行尝试安装，且这两种软件选择之一都会生成出错信息：

```
package xorg-x11-server-common has been added to the list of excluded packages, but it can't be removed from the current software selection without breaking the installation.
```

要临时解决这个问题，请不要在 **Server with GUI** 或 **Workstation** 软件选择中使用 CIS 安全配置集。

([BZ#1843932](#))

### 在 kickstart 安装过程中修复与服务相关的规则可能会失败

在 kickstart 安装过程中，OpenSCAP 工具有时会错误地显示服务的 **启用** 或 **禁用** 状态修正不需要。因此，OpenSCAP 可能会将安装的系统上的服务设置为不合规的状态。作为临时解决方案，您可以在 kickstart 安装后扫描并修复该系统。这可以解决与服务相关的问题。

([BZ#1834716](#))

### 某些 rsyslog 优先级字符串不能正常工作

对于允许对加密进行细粒度控制的 **imtcp** 的 **GnuTLS** 优先级字符串的支持尚未完成。因此，以下优先级字符串无法在 **rsyslog** 中正常工作：

```
NONE:+VERS-ALL:-VERS-TLS1.3:+MAC-ALL:+DHE-RSA:+AES-256-GCM:+SIGN-RSA-SHA384:+COMP-ALL:+GROUP-ALL
```

要临时解决这个问题，请只使用正确的优先级字符串：

```
NONE:+VERS-ALL:-VERS-TLS1.3:+MAC-ALL:+ECDHE-RSA:+AES-128-CBC:+SIGN-RSA-SHA1:+COMP-ALL:+GROUP-ALL
```

因此，当前的配置必须仅限于可正常工作的字符串。

([BZ#1679512](#))

### crypto-policies 错误地允许 Camellia 密码

RHEL 8 系统范围的加密策略应该在所有策略级别禁用 Camellia 密码，如产品文档中所述。但是 Kerberos 协议默认启用密码。

要临时解决这个问题，请应用 **NO-CAMELLIA** 子策略：

```
# update-crypto-policies --set DEFAULT:NO-CAMELLIA
```

在上个命令中，如果您之前已从 **DEFAULT** 进行了切换，请将 **DEFAULT** 替换为加密级别名称。

因此，只有在您通过临时解决方案禁用系统范围的加密策略的所有应用程序中，Camellia 密码才会被正确禁止。( [BZ#1919155](#) )

## 5.7.5. 网络

### iptables 程序现在为更新链的命令要求载入模块，而不会考虑 NLM\_F\_CREATE 标签

在以前的版本中，当设定链策略时，**iptables-nft** 程序会生成 **NEWCHAIN** 信息，但没有设置 **NLM\_F\_CREATE** 标志。因此，如果内核模块没有被手动加载，RHEL 8 内核不会加载任何模块，所得到的

update chain 命令会失败。有了这个更新，**iptables-nft** 工具现在为所有更新链的命令请求模块加载，用户可以使用 **iptables-nft** 工具设置链策略，而无需手动加载相关的模块。

(BZ#1812666)

### 对更新内核中的数据包/字节计数器的支持，在 RHEL 7 和 RHEL 8 之间被错误地更改了

当使用启用了 **iptables** 规则的计数器（即指定匹配 **ipset** 条目的额外约束）的 **ipset** 命令时，只有在所有附加约束匹配时才更新 **ipset** 计数器。在 **--packets-gt** 或 **--bytes-gt** 约束中存在问题。

因此，当将 **iptables** 规则集从 RHEL 7 迁移到 RHEL 8 时，涉及 **ipset** 查找的规则可能会停止工作，需要调整。要临时解决这个问题，请避免使用 **--packets-gt** 或 **--bytes-gt** 选项，并使用 **--packets-lt** 或者 **--bytes-lt** 选项替换它们。

(BZ#1806882)

### 在使用 nfp 驱动程序的 Netronome 网卡中卸载 XDP 程序失败

Netronome 网卡的 **nfp** 驱动程序存在 bug。因此，如果您使用这些卡，并使用带有 **XDP\_FLAGS\_REPLACE** 标志的 **IFLA\_XDP\_EXPECTED\_FD** 特性加载 XDP 程序时，卸载 eXpress Data Path(XDP)程序会失败。例如，这个程序错误会影响使用 **libxdp** 库载入的 XDP 程序。目前，这个问题还没有可用的临时解决方案。

(BZ#1880268)

### 在 ip 引导选项中使用 DHCP 时，Anaconda 没有网络访问权限

初始 RAM 磁盘(**initrd**)使用 NetworkManager 来管理网络。RHEL 8.3 ISO 文件提供的 **dracut** NetworkManager 模块错误地假设始终设置了 Anaconda 引导选项中 **ip** 选项的第一个字段。因此，如果您使用 DHCP 并设置 **ip=:::;<host\_name>::dhcp**，NetworkManager 将不会检索 IP 地址，并且网络在 Anaconda 中不可用。

您可以使用以下方法临时解决这个问题：

1. 将 **ip** 选项中的第一个字段设为 '.'：

```
ip=.:::;<host_name>::dhcp
```

请注意，当这个问题在以后的 RHEL 版本中被解决后，这个临时解决方案将不会起作用。

2. 使用包含错误修复的 BaseOS 存储库中的最新软件包重新创建 **boot.iso** 文件：

```
# lorax '--product=Red Hat Enterprise Linux' --version=8.3 --release=8.3 \
--source=<URL_to_BaseOS_repository> \
--source=<URL_to_AppStream_repository> \
--nomacboot --buildarch=x86_64 '--volid=RHEL 8.3' <output_directory>
```

.请注意，红帽不支持自创建的 ISO 文件。

因此，RHEL 可以从 DHCP 服务器获得 IP 地址，在 Anaconda 中可以访问网络。

(BZ#1902791)

## 5.7.6. 内核

### tboot-1.9.12-2 工具在 RHEL 8 中会导致引导失败

版本 1.9.12-2 的 **tboot** 工具会导致某些带有受信任的平台模块(TPM)2.0 的系统无法在旧模式下引导。因此，当系统尝试从 tboot Grand Unified Bootloader(GRUB)条目引导后会停止。要临时解决这个问题，请降级到 1.9.10 版本的 **tboot**。

(BZ#1947839)

### 内核在 IBM Z 系统中返回假的警告

在 RHEL 8 中，IBM Z 系统缺少 **ZONE\_DMA** 内存区的白名单条目来允许用户访问。因此，内核会返回假的警告，例如：

```
...
Bad or missing usercopy whitelist? Kernel memory exposure attempt detected from SLUB object
'dma-kmalloc-192' (offset 0, size 144)!
WARNING: CPU: 0 PID: 8519 at mm/usercopy.c:83 usercopy_warn+0xac/0xd8
...
```

当通过 **sysfs** 接口访问某些系统信息时会出现警告信息。例如，运行 **debuginfo.sh** 脚本。

要临时解决这个问题，在内核命令行中添加 **hardened\_usercopy=off** 参数。

因此，在以上场景中不会显示任何警告信息。

(BZ#1660290)

### rngd 服务忙等待会导致在 FIPS 模式下消耗掉所有 CPU

从版本 4.18.0-193.10 开始，内核添加了 FIPS 模式的新内核熵源。因此，当使用 FIPS 模式时，**rngd** 服务忙等待会等待对 **/dev/random** 设备的 **poll()** 系统调用，从而导致消耗掉 100% 的 CPU 时间。要临时解决这个问题，运行以下命令停止和禁用 **rngd**：

```
# systemctl stop rngd
# systemctl disable rngd
```

因此，在上述场景中，**rngd** 不再对 **poll()** 进行忙等待。

(BZ#1884857)

### softirq 更改会导致 localhost 接口在负载过重时丢弃 UDP 数据包

完成了对 Linux 内核的软件中断(**softirq**)处理的更改，以减少拒绝服务(DOS)的影响。因此，这导致了这样的情况，即 localhost 接口在负载过重时丢弃用户数据报协议(UDP)数据包。

要临时解决这个问题，将网络设备积压缓冲的大小增加到值 6000：

```
echo 6000 > /proc/sys/net/core/netdev_max_backlog
```

在红帽进行的测试中，这个值足以防止数据包丢失。负载较大的系统可能需要更大的积压值。增加的积压会导致潜在的延迟在 localhost 接口上增加。

结果是增加缓冲区并允许更多数据包等待处理，这降低了丢弃 localhost 数据包的几率。

(BZ#1779337)

### 在内存热插拔或拔出操作后，vmcore 捕获失败



执行内存 hot-plug 或 hot-unplug 操作后，会更新包含内存布局信息的设备树。因此，**makedumpfile** 实用程序会尝试访问不存在的物理地址。如果以下条件都满足，就会出现这个问题：

- IBM Power System 的 little-endian 变体运行 RHEL 8。
- 在系统中启用了 **kdump** 或者 **fadump** 服务。

因此，如果在内存 hot-plug 或 hot-unplug 操作后触发了内核崩溃，捕获内核将无法保存 **vmcore**。

要临时解决这个问题，在 hot-plug 或 hot-unplug 后重启 **kdump** 服务：

```
# systemctl restart kdump.service
```

因此，**vmcore** 在上述场景中被成功保存。

(BZ#1793389)

### 使用 **irqpoll** 会导致 **vmcore** 生成失败

由于在 Amazon Web Services(AWS)云平台上运行的 64 位 ARM 架构中的 **nvme** 驱动程序存在问题，在第一个内核提供了 **irqpoll** 内核命令行参数时 **vmcore** 生成会失败。因此，在内核崩溃后，**/var/crash/** 目录中不会转储 **vmcore** 文件。要临时解决这个问题：

1. 在 **/etc/sysconfig/kdump** 文件的 **KDUMP\_COMMANDLINE\_REMOVE** 键里添加 **irqpoll**。
2. 运行 **systemctl restart kdump** 命令重启 **kdump** 服务。

因此，第一个内核会正确引导，在内核崩溃时可以捕获 **vmcore** 文件。

请注意，**kdump** 服务可能会使用大量崩溃内核内存转储 **vmcore** 文件。确定捕获内核有足够的内存可用于 **kdump** 服务。

(BZ#1654962)

### Debug 内核无法在 RHEL 8 的崩溃捕获环境中引导

由于 debug 内核的内存需求特性，会在使用 debug 内核并触发内核 panic 时出现问题。因此，调试内核无法作为捕获内核引导，而是生成一个堆栈追踪。要临时解决这个问题，相应地增大崩溃内核内存。因此，debug 内核可以在崩溃捕获环境中成功引导。

(BZ#1659609)

### **zlib** 可能会在某些压缩功能中减慢 **vmcore** 捕获速度

**kdump** 配置文件默认使用 **lzo** 压缩格式 (**makedumpfile -l**)。当您修改使用 **zlib** 压缩格式 (**makedumpfile -c**) 的配置文件时，可能会带来更好的压缩效果，但会牺牲 **vmcore** 捕获过程的速度。因此，与 **lzo** 相比，捕获有 **zlib** 的 **vmcore** 文件所需的时间最多可能比使用 **kdump** 要长四倍。

因此，如果速度对您非常重要，红帽推荐使用默认的 **lzo**。但是，如果目标机器在可用空间中较低，**zlib** 就是一个更好的选项。

(BZ#1790635)

### HP NMI 监视器并不总是生成崩溃转储

在某些情况下，HP NMI watchdog 的 **hpwdt** 驱动无法声明一个由 HPE watchdog timer 生成的不可屏蔽中断 (NMI)，因为 NMI 被 **perfmon** 驱动所消耗。

缺少的 NMI 是由以下两个条件之一引发的：

1. Integrated Lights-Out (iLO) 服务器管理软件中的 **Generate NMI** 按钮。这个按钮由用户触发。
2. **hpwdt watchdog**。默认过期会向服务器发送一个 NMI。

在系统无响应时通常会出现这两个序列。在一般情况下，用于这两种情况的 NMI 处理程序调用 **kernel panic()** 功能，如果配置了，**kdump** 服务会生成 **vmcore** 文件。

由于缺少 NMI，没有调用 **kernel panic()** 且不收集 **vmcore**。

第一种情况(1.)，如果系统不响应，它会一直处于这个状态。要临时解决这种情况，请使用虚拟 **Power** 按钮来重置或者启用服务器。

在第二个示例中 (2.)，缺少的 NMI 之后会在 9 秒后被自动系统恢复 (ASR) 重置。

HPE Gen9 服务器行以单位数字显示这个问题。Gen10 频率更小。

(BZ#1602962)

### tuned-adm profile powerave 命令会导致系统变得无响应

执行 **tuned-adm profile powersave** 命令会导致具有旧的 Thunderx(CN88x)处理器的 Penguin Valkyrie 2000 2-socket 系统的无响应状态。因此，需要重启系统以便恢复工作。要临时解决这个问题，如果您的系统符合上述说明，请避免使用 **powersave** 配置集。

(BZ#1609288)

### 默认的 7 4 1 7 printk 值有时会导致临时系统无响应

默认的 **7 4 1 7 printk** 值可以更好地调试内核的活动。但是，当与串口控制台搭配使用时，这个 **printk** 设置可能会导致大量 I/O，从而导致 RHEL 系统暂时变得不响应。为了解决这个问题，添加了一个新的 **optimize-serial-console** TuneD 配置集，它把默认的 **printk** 值减为 **4 4 1 7**。用户可以按照以下方法追踪其系统：

```
# tuned-adm profile throughput-performance optimize-serial-console
```

重启后会保留一个较低的 **printk** 值，这可以降低系统挂起的可能性。

请注意，这个设置更改的代价是丢失额外的调试信息。

有关新添加的特性的更多信息，请参阅 [增加了一个新的 optimize-serial-console TuneD 配置集](#)，通过降低 **printk** 值来减小到串口控制台的 I/O。

(JIRA:RHELPLAN-28940)

### 内核 ACPI 驱动程序报告无法访问 PCIe ECAM 内存区域

固件提供的高级配置和电源接口 (ACPI) 表没有在 PCI 总线设备中定义内存区域。因此，在系统引导时会出现以下警告信息：

```
[ 2.817152] acpi PNP0A08:00: [Firmware Bug]: ECAM area [mem 0x30000000-0x31ffffff] not reserved in ACPI namespace
[ 2.827911] acpi PNP0A08:00: ECAM at [mem 0x30000000-0x31ffffff] for [bus 00-1f]
```

但是，内核仍然可以访问 **0x30000000-0x31ffff** 内存区域，并可以正确地将该内存区域分配给 PCI 增强配置访问机制(ECAM)。您可以通过以下输出通过 256 字节偏移访问 PCIe 配置空间来验证 PCI 是正常工作的：

```
03:00.0 Non-Volatile memory controller: Sandisk Corp WD Black 2018/PC SN720 NVMe SSD (prog-if 02 [NVM Express])
...
Capabilities: [900 v1] L1 PM Substates
    L1SubCap: PCI-PM_L1.2- PCI-PM_L1.1- ASPM_L1.2+ ASPM_L1.1- L1_PM_Substates+
    PortCommonModeRestoreTime=255us PortTPowerOnTime=10us
    L1SubCtl1: PCI-PM_L1.2- PCI-PM_L1.1- ASPM_L1.2- ASPM_L1.1-
    T_CommonMode=0us LTR1.2_Threshold=0ns
    L1SubCtl2: T_PwrOn=10us
```

因此，您可以忽略警告信息。

有关此问题的详情，请参阅 ["Firmware Bug: ECAM area mem 0x30000000-0x31ffff not reserved in ACPI namespace" appears during system boot.](#)

(BZ#1868526)

### OPEN MPI 库可能会使用默认 PML 的触发程序运行时失败

在 OPEN 消息密码界面 (OPEN MPI) 实现 4.0.x 系列中，Unified communicating X (UCX) 是默认的点到点通信器 (PML)。OPEN MPI 4.0.x 系列之后的版本弃用了 **openib** Byte Transfer Layer(BTL)。

但是，当 OPEN MPI 在 **同构** 集群 (相同的硬件和软件配置) 上运行时，UCX 仍会为 MPI 单边操作使用 **openib** BTL。因此，这可能会导致触发器执行错误。要临时解决这个问题：

- 使用以下参数运行 **mpirun** 命令：

```
-mca btl openib -mca pml ucx -x UCX_NET_DEVICES=mlx5_ib0
```

其中，

- **-mca btl openib** 参数禁用 **openib** BTL
- **-mca pml ucx** 参数将 OPEN MPI 配置为使用 **ucx** PML。
- **x UCX\_NET\_DEVICES=** 参数限制 UCX 使用指定的设备

OPEN MPI 在使用 **异构** 集群 (不同硬件和软件配置) 中运行时，使用 UCX 作为默认的 PML。因此，这可能会导致 OPEN MPI 任务在运行时出现错误的性能、不响应性行为或崩溃问题。要临时解决这个问题，将 UCX 优先级设置为：

- 使用以下参数运行 **mpirun** 命令：

```
-mca pml_ucx_priority 5
```

因此，OPEN MPI 库可以选择使用 UCX 的可替代传输层。

(BZ#1866402)

### 5.7.7. 文件系统和存储

无法将 **/boot** 文件系统放在 LVM 中

您不能将 **/boot** 文件系统放在 LVM 逻辑卷中。这种限制的原因如下：

- 在 EFI 系统中，*EFI 系统分区* 通常充当 **/boot** 文件系统。UEFI 标准要求有特定的 GPT 分区类型和具体文件系统类型。
- RHEL 8 在系统引导条目中使用 *Boot Loader 规格 (BLS)*。这个规格要求 **/boot** 文件系统可由平台固件可读。在 EFI 系统中，平台固件只能读取 uEFI 标准定义的 **/boot** 配置。
- 在 GRUB 2 引导装载程序中不支持 LVM 逻辑卷。红帽没有计划进行改进，因为如 uEFI 和 BLS 的标准，这个功能的使用情况正在下降。

红帽不计划在 LVM 中支持 **/boot**。反之，红帽提供了管理系统快照和回滚的工具，这些工具不需要将 **/boot** 文件系统放在 LVM 逻辑卷中。

(BZ#1496229)

### LVM 不再允许使用混合块大小创建卷组

LVM 工具（如 **vgcreate** 或 **vgextend**）不再允许您创建有不同逻辑块大小的物理卷（PV）的卷组（VG）。LVM 启用了这个更改，因为如果您使用不同块大小的 PV 扩展了基本逻辑卷（LV），文件系统将无法挂载。

要重新创建带有混合块大小的 VG，在 **lvm.conf** 文件中设置 **allow\_mixed\_block\_sizes=1** 选项。

(BZ#1768536)

### LVM writecache 的限制

**writecache** LVM 缓存方法有以下限制，这些限制不会出现在 **cache** 方法中：

- 使用 **pvmove** 命令时您无法命名 **writecache** 逻辑卷。
- 您不能将带有 **writecache** 的逻辑卷与精简池或 VDO 结合使用。

以下限制也适用于 **cache** 方法：

- 您不能在将 **cache** 或 **writecache** 附加到逻辑卷时重新定义大小。

(JIRA:RHELPLAN-27987、BZ#1798631、BZ#1808012)

### 保存一个 LUKS 卷的 LVM mirror 设备有时将变为无响应

在某些情况下，保存 LUKS 卷的片段类型的 **mirror** LVM 设备可能会变得无响应。无响应设备会拒绝所有 I/O 操作。

要解决这个问题，红帽建议在有弹性软件定义的存储之上使用带 **raid1** 的片段类型的 LVM RAID 1 设备而不是镜像 (**mirror**)。

**raid1** segment 类型是默认的 RAID 配置类型，它作为推荐的解决方案替换 **mirror**。

要将 **mirror** 设备转换为 **raid**，请参阅 [将镜像 LVM 设备转换为 RAID1 逻辑卷](#)。

(BZ#1730502)

### NFS 4.0 补丁可能会导致 open-heavy 工作负载性能降低。

在以前的版本中，存在一个程序错误，在某些情况下，可能会导致 NFS 打开操作覆盖文件已被删除或重命名在服务器中的事实。但是，这个修复可能会在需要很多打开操作的工作负载中造成性能下降。要临时解决这个问题，您可能需要使用 NFS 版本 4.1 或更高版本，这些版本已被改进为客户端在本地、快速和安

全地执行开放操作。

(BZ#1748451)

### 5.7.8. 动态编程语言、网页和数据库服务器

#### 当有 32 位应用程序调用 `getpwnam()` 时，可能会失败

当 NIS 用户使用 32 位应用程序调用 `getpwnam()` 函数时，如果没有 `nss_nis.i686` 软件包，则调用会失败。要临时解决这个问题，使用 `yum install nss_nis.i686` 手动安装缺少的软件包。

(BZ#1803161)

#### OpenLDAP 库之间的符号冲突可能会导致 `httpd` 中的崩溃

当 OpenLDAP 提供的 `libldap` 和 `libldap_r` 库被加载，并在单个进程中使用，这些库之间可能会出现符号冲突。因此，如果 `mod_security` 或 `mod_auth_openidc` 模块也是由 `httpd` 配置加载的，则使用 PHP `ldap` 扩展的 Apache `httpd` 子进程可能会意外终止。

有了这个对 Apache Portable Runtime (APR) 库的更新，您可以通过设置 `APR_DEEPCBIND` 环境变量来临时解决这个问题，该变量使在加载 `httpd` 模块时可以使用 `RTLD_DEEPCBIND` 动态链接器选项。当 `APR_DEEPCBIND` 环境变量启用时，崩溃不会在加载冲突库的 `httpd` 配置中发生。

(BZ#1819607)

#### PAM 插件无法在 MariaDB 中工作

**MariaDB 10.3** 提供了可插拔验证模块 (PAM) 插件版本 1.0。**MariaDB** PAM 插件版本 1.0 不能在 RHEL 8 中工作。要临时解决这个问题，请使用 `mariadb:10.5` 模块流提供的 PAM 插件版本 2.0，该模块流由 RHEL 8.4 提供。

(BZ#1942330)

### 5.7.9. 身份管理

#### 如果所有 KRA 成员都是隐藏的副本，则安装 KRA 会失败

如果在隐藏的副本中安装第一个 KRA 实例，`ipa-kra-install` 程序会在有密钥恢复授权 (KRA) 的集群中失败。因此，您无法向集群添加更多 KRA 实例。

要临时解决这个问题，请在添加新的 KRA 实例前，清除具有 KRA 角色的隐藏副本。`ipa-kra-install` 成功后您可以再次隐藏它。

(BZ#1816784)

#### 将 `cert-fix` 程序与 `--agent-uid pkidbuser` 选项一同使用会破坏证书系统

使用带有 `--agent-uid pkidbuser` 选项的 `cert-fix` 工具可破坏证书系统的 LDAP 配置。因此，证系统可能会变得不稳定，需要手动步骤才能恢复该系统。

(BZ#1729215)

#### 由连接到 PKI CA 的 PKI ACME Responder 发布的证书可能无法通过 OCSP 验证

PKI CA 提供的默认 ACME 证书配置文件包含一个示例 OCSP URL，其不指向实际的 OCSP 服务。因此，如果将 PKI ACME Responder 配置为使用 PKI CA 签发者，则响应者发布的证书可能会失败 OCSP 验证。

要临时解决这个问题，您需要在 `/usr/share/pki/ca/profiles/ca/acmeServerCert.cfg` 配置文件中将 `policyset.serverCertSet.5.default.params.authInfoAccessADLocation_0` 属性设置为空白值：

1. 在 ACME Responder 配置文件中，将行 `.serverCertSet.5.default.params.authInfoAccessADLocation_0=http://ocsp.example.com` 改为 `policyset.serverCertSet.5.default.params.authInfoAccessADLocation_0=`。
2. 重启服务并重新生成证书。

因此，PKI CA 将使用自动生成的 OCSP URL 生成 ACME 证书，指向实际 OCSP 服务。

(BZ#1868233)

## FreeRADIUS 会默默地截断大于 249 个字符的 Tunnel-Password

如果 Tunnel-Password 大于 249 个字符，则 FreeRADIUS 服务会默默地截断它。这可能导致无法预期的，与其它系统不兼容的密码。

要临时解决这个问题，请选择 249 个字符或更少的密码。

(BZ#1723362)

## IdM 主机上的 `/var/log/lastlog` 稀疏文件可能会导致性能问题

在 IdM 安装过程中，从总计 10,000 个可能范围内会随机选择并分配一个 200,000 UID 范围。当您决定以后合并两个独立的 IdM 域时，以这种方法选择一个随机范围可显著降低冲突 ID 的可能性。

但是，高 UID 可能会导致 `/var/log/lastlog` 文件出现问题。例如，如果 UID 为 1280000008 的用户登录到 IdM 客户端，则本地 `/var/log/lastlog` 文件的大小会增加到近 400 GB。虽然实际文件是稀疏的，且没有使用所有空间，但某些应用程序默认不是为识别稀疏文件而设计的，且可能需要一个特定的选项来处理这些文件。例如，如果设置比较复杂，备份和复制应用程序无法正确处理稀疏文件，则该文件会像大小为 400 GB 一样被复制。这个行为可能会导致性能问题。

要临时解决这个问题：

- 如果是标准软件包，请参考其文档来识别处理稀疏文件的选项。
- 如果是自定义应用程序，请确保它能够正确管理稀疏文件，如 `/var/log/lastlog`。

(JIRA:RHELPLAN-59111)

## 对 `ldap_id_use_start_tls` 选项使用默认值时的潜在风险

在使用没有 TLS 的 `ldap://` 进行身份查找时，可能会带来攻击向量的风险。特别是中间人(MITM)攻击，其允许攻击者，例如更改 LDAP 搜索中返回的对象的 UID 或 GID 来冒充用户。

目前，强制 TLS 的 SSSD 配置选项 `ldap_id_use_start_tls` 默认为 `false`。确保您的设置操作在可信环境中进行，并决定对 `id_provider = ldap` 使用未加密的通信是否是安全的。注意 `id_provider = ad` 和 `id_provider = ipa` 不受影响，因为它们使用 SASL 和 GSSAPI 保护的加密连接。

如果使用未加密的通信不安全，请在 `/etc/sss/sss.conf` 文件中将 `ldap_id_use_start_tls` 选项设置为 `true` 来强制使用 TLS。计划在以后的 RHEL 版本中更改的默认行为。

(JIRA:RHELPLAN-155168)

## 5.7.10. Desktop

### 无法从软件仓库中禁用 flatpak 程序库

目前，在 GNOME 软件工具中的软件程序库工具中无法禁用或删除 **flatpak** 程序库。

(BZ#1668760)

### 在桌面和应用程序间进行拖放操作无法正常工作

由于 **gnome-shell-extensions** 软件包中的一个 bug，drag-and-drop 功能目前在桌面和应用程序间无法正常工作。以后的发行版本中将重新添加对这个功能的支持。

(BZ#1717947)

### 第二代 RHEL 8 虚拟机有时无法在 Hyper-V Server 2016 主机上引导

当使用 RHEL 8 作为在 Microsoft Hyper-V Server 2016 主机上运行的虚拟机(VM)中的客户机操作系统时，虚拟机在某些情况下无法引导，并返回到 GRUB 引导菜单。另外，会在 Hyper-V 事件日志中记录以下错误：

```
The guest operating system reported that it failed with the following error code: 0x1E
```

这个错误是由 Hyper-V 主机上的 UEFI 固件错误造成的。要临时解决这个问题，使用 Hyper-V Server 2019 作为主机。

(BZ#1583445)

## 5.7.11. 图形基础结构

### radeon 无法正确重置硬件

**radeon** 内核驱动程序目前没有能在 kexec 上下文中正确重置硬件。相反，**radeon** 无法工作，从而导致剩余的 **kdump** 服务失败。

要临时解决这个问题，在 **kdump** 中禁用 **radeon**，方法是在 **/etc/kdump.conf** 文件中添加以下行：

```
dracut_args --omit-drivers "radeon"
force_rebuild 1
```

重启机器和 **kdump**。启动 **kdump** 后，**force\_rebuild 1** 行可能会从配置文件中删除。

请注意，在这种情况下，**kdump** 不会提供图形，但 **kdump** 可成功运行。

(BZ#1694705)

### 多个 HDR 显示在单个 MST 拓扑上可能无法打开

在使用带有 **nouveau** 驱动程序的 NVIDIA 图灵 GPU 的系统上，使用一个有支持 HDR 的多个显示器插入其中的 **DisplayPort** 集线器（如笔记本电脑底座），可能会导致打开失败。这是因为系统错误地认为 hub 中没有足够的带宽来支持所有显示器。

(BZ#1812577)

### 无法使用 **sudo** 命令运行图形应用程序

当试图以具有更高权限的用户运行图形应用程序时，应用程序无法打开并带有一个出错信息。发生故障的原因是 **Xwayland** 被 **Xauthority** 文件限制，为使用常规用户凭证进行验证。

要临时解决这个问题，使用 **sudo -E** 命令以 **root** 用户运行图形程序。

(BZ#1673073)

## VNC Viewer 显示在 IBM Z 中带有 16 位颜色深度的错误颜色

当您连接到带有 16 位色彩深度的 IBM Z 服务器上的 VNC 会话时，VNC Viewer 应用程序会显示错误的颜色。

要临时解决这个问题，请在 VNC 服务器中设置 24 位颜色深度。使用 **Xvnc** 服务器将 **-depth 16** 选项替换为 **-depth 24**（在 **Xvnc** 配置中）。

因此，VNC 客户端会显示正确的颜色，但在服务器中使用更多的网络带宽。

(BZ#1886147)

## ARM 不支持硬件加速

内置图形驱动程序不支持 64 位 ARM 架构中的硬件加速或 Vulkan API。

要启用硬件加速或者 ARM 上的 Vulkan，安装专有 Nvidia 驱动程序。

(JIRA:RHELPLAN-57914)

## RHEL 安装程序对 NVIDIA Ampere 没有响应

RHEL 8.3.0 不支持 NVIDIA Ampere GPU。如果您在具有 NVIDIA Ampere GPU 的系统上启动 RHEL 安装，则安装程序将没有响应。因此，安装无法成功完成。

NVIDIA Ampere 系列包括以下 GPU 型号：

- GeForce RTX 3060 Ti
- GeForce RTX 3070
- GeForce RTX 3080
- GeForce RTX 3090
- RTX A6000
- NVIDIA A40
- NVIDIA A100
- NVIDIA A100 80GB

要临时解决这个问题，请禁用 **nouveau** 图形驱动程序，并在文本模式下安装 RHEL：

1. 引导进入安装程序的引导菜单。
2. 在内核命令行上添加 **nouveau.modeset=0** 选项。  
详情请参阅 [编辑引导选项](#)。
3. 在系统上安装 RHEL。
4. 引导进入新安装的 RHEL。在引导菜单中，在内核命令行上添加 **nouveau.modeset=0** 选项。
5. 永久禁用 **nouveau** 驱动程序：

```
# echo 'blacklist nouveau' >> /etc/modprobe.d/blacklist.conf
```



作为结果，安装会成功完成，RHEL 现在以文本模式运行。

另外，您可以安装专有 NVIDIA GPU 驱动程序以启用图形。具体步骤请参阅[如何在 RHEL 8 中安装 NVIDIA 专有驱动程序](#)。

(BZ#1903890)

## 5.7.12. Web 控制台

### 非特权用户可以访问订阅页面

如果非管理员访问 web 控制台的 **Subscriptions** 页面，Web 控制台会显示一个通用错误消息 **Cockpit had an unexpected internal error**。

要临时解决这个问题，使用特权用户登录到 web 控制台，并选择 **Reuse my password for privileged tasks** 复选框。

(BZ#1674337)

## 5.7.13. Red Hat Enterprise Linux 系统角色

### System Roles Logging 不支持 oVirt 输入和 elasticsearch 输出功能

系统角色日志中不支持 **oVirt** 输入和 **elasticsearch** 输出，虽然 README 文件中已提到它们。目前还没有可用的临时解决方案。

(BZ#1889468)

## 5.7.14. 虚拟化

### 无法通过 QXL 显示多个使用 Wayland 的虚拟机的监控器

使用 **remote-viewer** 工具来显示使用 Wayland 显示服务器的虚拟机(VM)的多个显示器，会导致 VM 变得无响应，并永久显示 *Waiting for display* 状态信息。

要临时解决这个问题，使用 **virtio-gpu** 而不是 **qxl** 作为使用 Wayland 的虚拟机的 GPU 设备。

(BZ#1642887)

### virsh iface-\* 命令无法一致性地工作

因为配置的依赖关系，目前 **virsh iface-\*** 命令（如 **virsh iface-start** 和 **virsh iface-destroy** 会经常失败。因此，建议您不要使用 **virsh iface-\*** 命令配置和管理主机网络连接。反之，使用 NetworkManager 程序及其相关管理程序。

(BZ#1664592)

### 当使用很多 virtio-blk 磁盘时，虚拟机有时无法启动

在虚拟机(VM)中添加大量 **virtio-blk** 设备可能会耗尽平台中可用的中断向量。如果发生了这种情况，VM 的客户机操作系统无法引导，并显示 **dracut-initqueue[392]: Warning: Could not boot** 错误。

(BZ#1719687)

### 使用 virtio-blk 将 LUN 设备附加到虚拟机中无法正常工作

q35 机器类型不支持 virtio 1.0 设备，因此 RHEL 8 不支持 virtio 1.0 中弃用的功能。特别是，RHEL 8 主机无法从 virtio-blk 设备发送 SCSI 命令。因此，使用 virtio-blk 控制器时，将物理磁盘作为 LUN 设备附加到虚拟机会失败。

请注意，物理磁盘仍可被传递给客户端操作系统，但应该使用 **device='disk'** 选项而不是 **device='lun'** 选项进行配置。

(BZ#1777138)

### 当主机上禁用 TSX 时，使用 Cooperlake 的虚拟机无法引导

使用 **Cooperlake** CPU 模型的虚拟机 (VM) 目前在主机上禁用 **TSX** CPU 标签时无法引导。相反，主机将显示以下出错信息：

```
the CPU is incompatible with host CPU: Host CPU does not provide required features: hle, rtm
```

要在此类主机上使用 **Cooperlake** 生成虚拟机，请在虚拟机 XML 配置中禁用 VM 配置中的 HLE、RTM 和 TAA\_NO 标志：

```
<feature policy='disable' name='hle'/>
<feature policy='disable' name='rtm'/>
<feature policy='disable' name='taa-no'/>
```

(BZ#1860743)

### 虚拟机有时无法在 Witherspoon 主机上引导

在某些情况下，使用 **pseries-rhel7.6.0-sxxm** 机器类型的虚拟机(VM)不能在使用 DD2.2 或 DD2.3 CPU 的 *Power9 S922LC for HPC* 主机上启动。

尝试引导这样的虚拟机会生成以下出错信息：

```
qemu-kvm: Requested safe indirect branch capability level not supported by kvm
```

要临时解决这个问题，请配置虚拟机的 XML 配置，如下所示：

```
<domain type='qemu' xmlns:qemu='http://libvirt.org/schemas/domain/qemu/1.0'>
  <qemu:commandline>
    <qemu:arg value='-machine'/>
    <qemu:arg value='cap-ibs=workaround'/>
  </qemu:commandline>
```

(BZ#1732726)

## 5.7.15. 云环境中的 RHEL

### Azure NV6 实例上的 GPU 问题

当在 Microsoft Azure NV6 实例上运行 RHEL 8 作为客户机操作系统时，从休眠状态恢复虚拟机 (VM) 有时会导致虚拟机的 GPU 工作不正确。当发生这种情况时，内核会记录以下信息：

```
hv_irq_unmask() failed: 0x5
```

(BZ#1846838)

## kdump 有时不会在 Azure 和 Hyper-V 上启动

在托管在 Microsoft Azure 或 Hyper-V hypervisor 上的 RHEL 8 客户机操作系统中，启动 **kdump** 内核在某些情况下会在启用执行后通知程序时失败。

要临时解决这个问题，请禁用 `crash kexec post notifiers`：

```
# echo N > /sys/module/kernel/parameters/crash_kexec_post_notifiers
```

(BZ#1865745)

## 在 VMWare 主机的 RHEL 8 虚拟机中设置静态 IP 无法正常工作

目前，当在 VMWare 主机中使用 RHEL 8 作为虚拟机 (VM) 的客户机操作系统时，`DatasourceOVF` 功能无法正常工作。因此，如果您使用 `cloud-init` 程序将虚拟机的网络设置为静态 IP，然后重启虚拟机，则虚拟机的网络将变为 DHCP。

(BZ#1750862)

## 内核转储带有特定 NIC 的 RHEL 8 虚拟机到 Azure 的远程机器所需的时间比预期的时间要长

目前，虚拟机使用启用了加速网络的 NIC 时，用 **kdump** 实用程序将 RHEL 8 虚拟机 (VM) 的内核转储保存到远程机器上无法正常工作。因此，转储文件会在大约 200 秒后保存，而不是立即保存。另外，在保存转储文件前会在控制台中记录以下出错信息。

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

(BZ#1854037)

## 在虚拟机从休眠中恢复后，TX/RX 数据包计数器不会增加

在 Microsoft Azure 上恢复休眠时，当 RHEL 8 虚拟机 (VM) 使用 CX4 VF NIC 时，**TX/RX** 数据包计数器会停止增长。要让计数器保持工作正常，重启虚拟机。请注意，这样做会重置计数器。

(BZ#1876527)

## RHEL 8 虚拟机无法从 Azure 的休眠状态恢复

当启用 **SR-IOV** 的 RHEL 8 虚拟机 (VM) 已休眠并在 Microsoft Azure 上被取消分配，则虚拟功能 (VF) (`vmbus` 设备) 的 GUID 会改变。因此，当虚拟机被重启时，它无法恢复并崩溃。作为临时解决方案，使用 Azure 串口控制台硬重置虚拟机。

(BZ#1876519)

## 将 POWER9 客户端从 RHEL 7-ALT 主机迁移到 RHEL 8 会失败

目前，将 POWER9 虚拟机从 RHEL 7-ALT 主机系统迁移到 RHEL 8 会变得无响应，状态为 "Migration status: active"。

要临时解决这个问题，在 RHEL 7-ALT 主机上禁用 Transparent Huge Pages (THP)，这样可使迁移成功完成。

(BZ#1741436)

## 5.7.16. 支持性

### redhat-support-tool 无法用于 FUTURE 加密策略

因为客户门户网站 API 中的证书使用的加密密钥不满足 **FUTURE** 系统范围的加密策略的要求，所以 **redhat-support-tool** 程序目前无法使用这个策略级别。

要临时解决这个问题，在连接到客户门户网站 API 时使用 **DEFAULT** 加密策略。

([BZ#1802026](#))

## 5.7.17. 容器

### UDICA 无法与 1.0 稳定流工作

UDICA，为容器生成 SELinux 策略的工具，不能与通过 **container-tools:1.0** 模块流中的 podman 1.0.x 运行的容器一起使用。

([JIRA:RHELPLAN-25571](#))

### podman system connection add 不会自动设置默认连接

**podman system connection add** 命令不会自动将第一个连接设置为默认连接。要设置默认连接，您必须手动运行命令 **podman system connection default <connection\_name>**。

([BZ#1881894](#))

## 第 6 章 国际化

### 6.1. RED HAT ENTERPRISE LINUX 8 国际语言

Red Hat Enterprise Linux 8 支持多种语言的安装，并根据您的需要更改语言。

- 东亚语言 - 日语、韩语、简体中文和繁体中文。
- 欧洲语言 - 英语、德语、西班牙语、法语、意大利语、葡萄牙语和俄语。

下表列出了为各种主要语言提供的字体和输入法。

语言	默认字体（字体软件包）	输入法
English	dejavu-sans-fonts	
法语	dejavu-sans-fonts	
德语	dejavu-sans-fonts	
意大利语	dejavu-sans-fonts	
俄语	dejavu-sans-fonts	
西班牙语	dejavu-sans-fonts	
葡萄牙语	dejavu-sans-fonts	
简体中文	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-libpinyin, libpinyin
繁体中文	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-libzhuyin, libzhuyin
日语	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-kkc, libkc
韩语	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-hangul, libhangul

### 6.2. RHEL 8 国际化的显著变化

RHEL 8 与 RHEL 7 相比，对国际化进行了以下更改：

- 添加了对 **Unicode 11** 计算行业标准的支持。
- 国际化发布在多个软件包中，这样就可以进行较小的内存占用安装。如需更多信息，请参阅 [使用语言包](#)。
- 很多 **glibc** 区域已经与 Unicode Common Locale Data Repository (CLDR) 同步。

## 附录 A. 按组件划分的问题单列表

Bugzilla 和 JIRA ID 列在本文档中以便参考。可公开访问的 Bugzilla 程序错误包括到 ticket 的链接。

组件	票证
<b>389-ds-base</b>	<a href="#">BZ#1816862</a> , <a href="#">BZ#1638875</a> , <a href="#">BZ#1728943</a>
<b>NetworkManager</b>	<a href="#">BZ#1814746</a> , <a href="#">BZ#1626348</a>
<b>anaconda</b>	<a href="#">BZ#1665428</a> , <a href="#">BZ#1775975</a> , <a href="#">BZ#1630299</a> , <a href="#">BZ#1823578</a> , <a href="#">BZ#1672405</a> , <a href="#">BZ#1644662</a> , <a href="#">BZ#1745064</a> , <a href="#">BZ#1821192</a> , <a href="#">BZ#1822880</a> , <a href="#">BZ#1862116</a> , <a href="#">BZ#1890261</a> , <a href="#">BZ#1891827</a> , <a href="#">BZ#1691319</a> , <a href="#">BZ#1931069</a>
<b>apr</b>	<a href="#">BZ#1819607</a>
<b>authselect</b>	<a href="#">BZ#1654018</a>
<b>bcc</b>	<a href="#">BZ#1837906</a>
<b>bind</b>	<a href="#">BZ#1818785</a>
<b>buildah-container</b>	<a href="#">BZ#1627898</a>
<b>buildah</b>	<a href="#">BZ#1806044</a>
<b>clevis</b>	<a href="#">BZ#1716040</a> , <a href="#">BZ#1818780</a> , <a href="#">BZ#1436735</a> , <a href="#">BZ#1819767</a>
<b>cloud-init</b>	<a href="#">BZ#1750862</a>
<b>cloud-utils-growpart</b>	<a href="#">BZ#1846246</a>
<b>cockpit-session-recording</b>	<a href="#">BZ#1826516</a>
<b>cockpit</b>	<a href="#">BZ#1710731</a> , <a href="#">BZ#1666722</a>
<b>corosync-qdevice</b>	<a href="#">BZ#1784200</a>
<b>crun</b>	<a href="#">BZ#1841438</a>
<b>crypto-policies</b>	<a href="#">BZ#1832743</a> , <a href="#">BZ#1660839</a>
<b>cyrus-sasl</b>	<a href="#">BZ#1817054</a>
<b>distribution</b>	<a href="#">BZ#1815402</a> , <a href="#">BZ#1657927</a>
<b>dnf</b>	<a href="#">BZ#1793298</a> , <a href="#">BZ#1832869</a> , <a href="#">BZ#1842285</a>

组件	票证
<b>elfutils</b>	<a href="#">BZ#1804321</a>
<b>fapolicyd</b>	<a href="#">BZ#1897090</a> , <a href="#">BZ#1817413</a> , <a href="#">BZ#1714529</a>
<b>fence-agents</b>	<a href="#">BZ#1830776</a> , <a href="#">BZ#1775847</a>
<b>firewalld</b>	<a href="#">BZ#1790948</a> , <a href="#">BZ#1682913</a> , <a href="#">BZ#1809225</a> , <a href="#">BZ#1817205</a> , <a href="#">BZ#1809636</a>
<b>freeradius</b>	<a href="#">BZ#1672285</a> , <a href="#">BZ#1859527</a> , <a href="#">BZ#1723362</a>
<b>gcc-toolset-10-gdb</b>	<a href="#">BZ#1838777</a>
<b>gcc</b>	<a href="#">BZ#1784758</a>
<b>gdb</b>	<a href="#">BZ#1659535</a>
<b>git</b>	<a href="#">BZ#1825114</a>
<b>glibc</b>	<a href="#">BZ#1812756</a> , <a href="#">BZ#1743445</a> , <a href="#">BZ#1783303</a> , <a href="#">BZ#1642150</a> , <a href="#">BZ#1810146</a> , <a href="#">BZ#1748197</a> , <a href="#">BZ#1774115</a> , <a href="#">BZ#1807824</a> , <a href="#">BZ#1757354</a> , <a href="#">BZ#1836867</a> , <a href="#">BZ#1780204</a> , <a href="#">BZ#1821531</a> , <a href="#">BZ#1784525</a>
<b>gnome-session</b>	<a href="#">BZ#1739556</a>
<b>gnome-shell-extensions</b>	<a href="#">BZ#1717947</a>
<b>gnome-shell</b>	<a href="#">BZ#1724302</a>
<b>gnome-software</b>	<a href="#">BZ#1668760</a>
<b>gnutls</b>	<a href="#">BZ#1677754</a> , <a href="#">BZ#1789392</a> , <a href="#">BZ#1849079</a> , <a href="#">BZ#1855803</a>
<b>go-toolset</b>	<a href="#">BZ#1820596</a>
<b>gpgme</b>	<a href="#">BZ#1829822</a>
<b>grafana-container</b>	<a href="#">BZ#1823834</a>
<b>grafana-pcp</b>	<a href="#">BZ#1807099</a>
<b>grafana</b>	<a href="#">BZ#1807323</a>
<b>grub2</b>	<a href="#">BZ#1583445</a>
<b>httpd</b>	<a href="#">BZ#1209162</a>

组件	票证
<b>initial-setup</b>	<a href="#">BZ#1676439</a>
<b>ipa-healthcheck</b>	<a href="#">BZ#1852244</a>
<b>ipa</b>	<a href="#">BZ#1816784</a> , <a href="#">BZ#1810154</a> , <a href="#">BZ#913799</a> , <a href="#">BZ#1651577</a> , <a href="#">BZ#1851139</a> , <a href="#">BZ#1664719</a> , <a href="#">BZ#1664718</a>
<b>iperf3</b>	<a href="#">BZ#1665142</a> , <a href="#">BZ#1700497</a>
<b>jss</b>	<a href="#">BZ#1821851</a>
<b>kernel-rt</b>	<a href="#">BZ#1818138</a>
<b>kernel</b>	<a href="#">BZ#1758323</a> , <a href="#">BZ#1812666</a> , <a href="#">BZ#1793389</a> , <a href="#">BZ#1694705</a> , <a href="#">BZ#1748451</a> , <a href="#">BZ#1654962</a> , <a href="#">BZ#1792125</a> , <a href="#">BZ#1708456</a> , <a href="#">BZ#1812577</a> , <a href="#">BZ#1757933</a> , <a href="#">BZ#1847837</a> , <a href="#">BZ#1791664</a> , <a href="#">BZ#1666538</a> , <a href="#">BZ#1602962</a> , <a href="#">BZ#1609288</a> , <a href="#">BZ#1730502</a> , <a href="#">BZ#1806882</a> , <a href="#">BZ#1660290</a> , <a href="#">BZ#1846838</a> , <a href="#">BZ#1865745</a> , <a href="#">BZ#1868526</a> , <a href="#">BZ#1884857</a> , <a href="#">BZ#1854037</a> , <a href="#">BZ#1876527</a> , <a href="#">BZ#1876519</a> , <a href="#">BZ#1823764</a> , <a href="#">BZ#1822085</a> , <a href="#">BZ#1735611</a> , <a href="#">BZ#1281843</a> , <a href="#">BZ#1828642</a> , <a href="#">BZ#1825414</a> , <a href="#">BZ#1761928</a> , <a href="#">BZ#1791041</a> , <a href="#">BZ#1796565</a> , <a href="#">BZ#1834769</a> , <a href="#">BZ#1785660</a> , <a href="#">BZ#1683394</a> , <a href="#">BZ#1817752</a> , <a href="#">BZ#1782831</a> , <a href="#">BZ#1821646</a> , <a href="#">BZ#1519039</a> , <a href="#">BZ#1627455</a> , <a href="#">BZ#1501618</a> , <a href="#">BZ#1495358</a> , <a href="#">BZ#1633143</a> , <a href="#">BZ#1503672</a> , <a href="#">BZ#1570255</a> , <a href="#">BZ#1696451</a> , <a href="#">BZ#1348508</a> , <a href="#">BZ#1778762</a> , <a href="#">BZ#1839311</a> , <a href="#">BZ#1783396</a> , <a href="#">BZ#1665295</a> , <a href="#">BZ#1658840</a> , <a href="#">BZ#1660627</a> , <a href="#">BZ#1569610</a>
<b>krb5</b>	<a href="#">BZ#1791062</a> , <a href="#">BZ#1784655</a> , <a href="#">BZ#1820311</a> , <a href="#">BZ#1802334</a> , <a href="#">BZ#1877991</a>
<b>libbpf</b>	<a href="#">BZ#1759154</a>
<b>libcap</b>	<a href="#">BZ#1487388</a>
<b>libdb</b>	<a href="#">BZ#1670768</a>
<b>libffi</b>	<a href="#">BZ#1723951</a>
<b>libgnome-keyring</b>	<a href="#">BZ#1607766</a>
<b>libkcapi</b>	<a href="#">BZ#1683123</a>
<b>libmaxminddb</b>	<a href="#">BZ#1642001</a>
<b>libpcap</b>	<a href="#">BZ#1806422</a>
<b>libreswan</b>	<a href="#">BZ#1544463</a> , <a href="#">BZ#1820206</a>



组件	票证
libseccomp	<a href="#">BZ#1770693</a>
libselinux-python-2.8-module	BZ#1666328
libssh	<a href="#">BZ#1804797</a>
libvirt	BZ#1664592, BZ#1528684
lldb	BZ#1841073
llvm-toolset	BZ#1820587
llvm	BZ#1820319
lshw	<a href="#">BZ#1794049</a>
lvmm2	BZ#1496229, <a href="#">BZ#1768536</a> , BZ#1598199, BZ#1541165, JIRA:RHELPLAN-39320
mariadb	<a href="#">BZ#1942330</a>
memcached	<a href="#">BZ#1809536</a>
mesa	<a href="#">BZ#1886147</a>
microdnf	<a href="#">BZ#1781126</a>
mod_http2	<a href="#">BZ#1814236</a>
nfs-utils	<a href="#">BZ#1817756</a> , BZ#1592011
nginx	<a href="#">BZ#1668717</a> , <a href="#">BZ#1826632</a>
nmstate	BZ#1674456
nss_nis	<a href="#">BZ#1803161</a>
nss	<a href="#">BZ#1817533</a> , BZ#1645153
opencryptoki	BZ#1780293
openmpi	BZ#1866402
opensc	<a href="#">BZ#1810660</a>

组件	票证
<b>openscap</b>	<a href="#">BZ#1803116</a> , <a href="#">BZ#1870087</a> , <a href="#">BZ#1795563</a> , <a href="#">BZ#1824152</a> , <a href="#">BZ#1829761</a>
<b>openssh</b>	<a href="#">BZ#1744108</a>
<b>openssl</b>	<a href="#">BZ#1685470</a> , <a href="#">BZ#1810911</a>
<b>oscap-anaconda-addon</b>	<a href="#">BZ#1816199</a> , <a href="#">BZ#1665082</a> , <a href="#">BZ#1674001</a> , <a href="#">BZ#1691305</a> , <a href="#">BZ#1787156</a> , <a href="#">BZ#1843932</a> , <a href="#">BZ#1834716</a>
<b>pacemaker</b>	<a href="#">BZ#1828488</a> , <a href="#">BZ#1784601</a> , <a href="#">BZ#1837747</a> , <a href="#">BZ#1718324</a>
<b>papi</b>	<a href="#">BZ#1807346</a> , <a href="#">BZ#1664056</a> , <a href="#">BZ#1726070</a>
<b>pcp-container</b>	<a href="#">BZ#1497296</a>
<b>pcp</b>	<a href="#">BZ#1792971</a>
<b>pcs</b>	<a href="#">BZ#1817547</a> , <a href="#">BZ#1684676</a> , <a href="#">BZ#1839637</a> , <a href="#">BZ#1619620</a>
<b>perl-5.30-module</b>	<a href="#">BZ#1713592</a>
<b>perl-IO-Socket-SSL</b>	<a href="#">BZ#1824222</a>
<b>perl-libwww-perl</b>	<a href="#">BZ#1781177</a>
<b>php</b>	<a href="#">BZ#1797661</a>
<b>pki-core</b>	<a href="#">BZ#1729215</a> , <a href="#">BZ#1868233</a> , <a href="#">BZ#1770322</a> , <a href="#">BZ#1824948</a>
<b>podman</b>	<a href="#">BZ#1804193</a> , <a href="#">BZ#1881894</a> , <a href="#">BZ#1627899</a>
<b>powertop</b>	<a href="#">BZ#1783110</a>
<b>pykickstart</b>	<a href="#">BZ#1637872</a>
<b>python38</b>	<a href="#">BZ#1847416</a>
<b>qemu-kvm</b>	<a href="#">BZ#1719687</a> , <a href="#">BZ#1860743</a> , <a href="#">JIRA:RHELPLAN-45901</a> , <a href="#">BZ#1651994</a>
<b>rear</b>	<a href="#">BZ#1843809</a> , <a href="#">BZ#1729502</a> , <a href="#">BZ#1743303</a>
<b>redhat-support-tool</b>	<a href="#">BZ#1802026</a>
<b>resource-agents</b>	<a href="#">BZ#1814896</a>

组件	票证
<b>rhel-system-roles-sap</b>	<a href="#">BZ#1844190</a> , <a href="#">BZ#1660832</a>
<b>rhel-system-roles</b>	<a href="#">BZ#1889468</a> , <a href="#">BZ#1822158</a> , <a href="#">BZ#1677739</a>
<b>rpm</b>	<a href="#">BZ#1688849</a>
<b>rsyslog</b>	<a href="#">BZ#1659383</a> , <a href="#">JIRA:RHELPLAN-10431</a> , <a href="#">BZ#1679512</a> , <a href="#">BZ#1713427</a>
<b>ruby-2.7-module</b>	<a href="#">BZ#1817135</a>
<b>Ruby</b>	<a href="#">BZ#1846113</a>
<b>rust-toolset</b>	<a href="#">BZ#1820593</a>
<b>samba</b>	<a href="#">BZ#1817557</a> , <a href="#">JIRA:RHELPLAN-13195</a>
<b>scap-security-guide</b>	<a href="#">BZ#1843913</a> , <a href="#">BZ#1858866</a> , <a href="#">BZ#1750755</a> , <a href="#">BZ#1760734</a> , <a href="#">BZ#1832760</a> , <a href="#">BZ#1815007</a>
<b>scap-workbench</b>	<a href="#">BZ#1640715</a>
<b>selinux-policy</b>	<a href="#">BZ#1826788</a> , <a href="#">BZ#1746398</a> , <a href="#">BZ#1776873</a> , <a href="#">BZ#1772852</a> , <a href="#">BZ#1641631</a> , <a href="#">BZ#1860443</a>
<b>setools</b>	<a href="#">BZ#1820079</a>
<b>skopeo-container</b>	<a href="#">BZ#1627900</a>
<b>smartmontools</b>	<a href="#">BZ#1671154</a>
<b>spice</b>	<a href="#">BZ#1849563</a>
<b>squid</b>	<a href="#">BZ#1829467</a>
<b>sssd</b>	<a href="#">BZ#1827615</a> , <a href="#">BZ#1793727</a>
<b>stratis-cli</b>	<a href="#">BZ#1734496</a>
<b>stunnel</b>	<a href="#">BZ#1808365</a>
<b>subscription-manager</b>	<a href="#">BZ#1674337</a>
<b>sudo</b>	<a href="#">BZ#1786990</a>
<b>systemtap</b>	<a href="#">BZ#1804319</a>

组件	票证
<b>tang</b>	<a href="#">BZ#1716039</a>
<b>tcpdump</b>	<a href="#">BZ#1804063</a>
<b>tigervnc</b>	<a href="#">BZ#1806992</a>
<b>tpm2-tools</b>	<a href="#">BZ#1789682</a>
<b>tuned</b>	<a href="#">BZ#1792264</a> , <a href="#">BZ#1840689</a> , <a href="#">BZ#1746957</a>
<b>udica</b>	<a href="#">BZ#1763210</a>
<b>usbguard</b>	<a href="#">BZ#1738590</a> , <a href="#">BZ#1667395</a> , <a href="#">BZ#1683567</a>
<b>valgrind</b>	<a href="#">BZ#1804324</a>
<b>wayland</b>	<a href="#">BZ#1673073</a>
<b>xdp-tools</b>	<a href="#">BZ#1880268</a> , <a href="#">BZ#1820670</a>
<b>xorg-x11-drv-qxl</b>	<a href="#">BZ#1642887</a>
<b>xorg-x11-server</b>	<a href="#">BZ#1698565</a>
<b>yum</b>	<a href="#">BZ#1788154</a>

组件	票证
其他	<p>JIRA:RHELPLAN-45950, JIRA:RHELPLAN-57572, BZ#1640697, BZ#1659609, <a href="#">BZ#1687900</a>, BZ#1697896, BZ#1790635, BZ#1823398, BZ#1757877, JIRA:RHELPLAN-25571, BZ#1777138, JIRA:RHELPLAN-27987, JIRA:RHELPLAN-28940, JIRA:RHELPLAN-34199, JIRA:RHELPLAN-57914, <a href="#">BZ#1897383</a>, <a href="#">BZ#1900019</a>, <a href="#">BZ#1839151</a>, <a href="#">BZ#1780124</a>, JIRA:RHELPLAN-42395, <a href="#">BZ#1889736</a>, BZ#1842656, JIRA:RHELPLAN-45959, JIRA:RHELPLAN-45958, JIRA:RHELPLAN-45957, JIRA:RHELPLAN-45956, JIRA:RHELPLAN-45952, JIRA:RHELPLAN-45945, JIRA:RHELPLAN-45939, JIRA:RHELPLAN-45937, JIRA:RHELPLAN-45936, JIRA:RHELPLAN-45930, JIRA:RHELPLAN-45926, JIRA:RHELPLAN-45922, JIRA:RHELPLAN-45920, JIRA:RHELPLAN-45918, JIRA:RHELPLAN-45916, JIRA:RHELPLAN-45915, JIRA:RHELPLAN-45911, JIRA:RHELPLAN-45910, JIRA:RHELPLAN-45909, JIRA:RHELPLAN-45908, JIRA:RHELPLAN-45906, JIRA:RHELPLAN-45904, JIRA:RHELPLAN-45900, JIRA:RHELPLAN-45899, JIRA:RHELPLAN-45884, JIRA:RHELPLAN-37573, JIRA:RHELPLAN-37570, JIRA:RHELPLAN-49954, JIRA:RHELPLAN-50002, JIRA:RHELPLAN-43531, JIRA:RHELPLAN-48838, <a href="#">BZ#1873567</a>, <a href="#">BZ#1866695</a>, JIRA:RHELPLAN-14068, JIRA:RHELPLAN-7788, JIRA:RHELPLAN-40469, JIRA:RHELPLAN-42617, JIRA:RHELPLAN-30878, JIRA:RHELPLAN-37517, JIRA:RHELPLAN-55009, JIRA:RHELPLAN-42396, BZ#1836211, JIRA:RHELPLAN-57564, JIRA:RHELPLAN-57567, <a href="#">BZ#1890499</a>, JIRA:RHELPLAN-40234, JIRA:RHELPLAN-56676, JIRA:RHELPLAN-14754, JIRA:RHELPLAN-51289, <a href="#">BZ#1893174</a>, BZ#1690207, JIRA:RHELPLAN-1212, BZ#1559616, <a href="#">BZ#1889737</a>, <a href="#">BZ#1812552</a>, JIRA:RHELPLAN-14047, <a href="#">BZ#1769727</a>, JIRA:RHELPLAN-27394, JIRA:RHELPLAN-27737, JIRA:RHELPLAN-41549, BZ#1642765, JIRA:RHELPLAN-10304, BZ#1646541, BZ#1647725, <a href="#">BZ#1686057</a>, <a href="#">BZ#1748980</a>, BZ#1827628, <a href="#">BZ#1871025</a>, <a href="#">BZ#1871953</a>, BZ#1874892, <a href="#">BZ#1893767</a>, JIRA:RHELPLAN-60226</p>

## 附录 B. 修订历史

### 0.3-9

2023 年 12 月 7 日星期四, Lucie Vaááková([lvarakova@redhat.com](mailto:lvarakova@redhat.com))

- 添加了一个已弃用的功能 [JIRA:RHELDOCS-16612](#) (身份管理)。

### 0.3-8

2023 年 11 月 10 日星期五, Gabriela Fialová([gfialova@redhat.com](mailto:gfialova@redhat.com))

- 更新了 RHEL 文档中的提供反馈模块。

### 0.3-7

2023 年 11 月 7 日星期二, Gabriela Fialová([gfialova@redhat.com](mailto:gfialova@redhat.com))

- 修复损坏的链接。

### 0.3-6

2023 年 10 月 13 日星期五, Gabriela Fialová([gfialova@redhat.com](mailto:gfialova@redhat.com))

- 添加了一个技术预览 [JIRA:RHELDOCS-16861](#) (容器)。

### 0.3-5

2023 年 4 月 27 日星期四, Gabriela Fialová([gfialova@redhat.com](mailto:gfialova@redhat.com))

- 添加了一个已知问题 [JIRA:RHELPLAN-155168](#) (身份管理)。

### 0.3-4

2022 年 4 月 29 日星期五, Lenka Špačková ([lspackova@redhat.com](mailto:lspackova@redhat.com))

- 更新了已弃用的功能简介。
- 修复了 [BZ#1605216](#) 中的拼写错误。
- 修复了损坏的链接。

### 0.3-3

2022 年 4 月 5 日 星期二, Jaroslav Klech([jklech@redhat.com](mailto:jklech@redhat.com))

- 添加了 bug 修复 [BZ#1666538](#) (内核)。

### 0.3-2

2022 年 3 月 17 日 星期四, Jroslav Klech([jklech@redhat.com](mailto:jklech@redhat.com))

- 添加了已知问题(内核)。

### 0.3-1

2022 年 2 月 4 日 星期五, Lucie Maňásková ([لمانasko@redhat.com](mailto:لمانasko@redhat.com))

- 添加了已弃用的功能 [BZ#1794513](#) (文件系统和存储)。

### 0.3-0

2021 年 12 月 23 日星期四, Lenka Paová([lspackova@redhat.com](mailto:lspackova@redhat.com))

- 向技术预览 [BZ#1605216](#) 和已弃用的功能 [BZ#1878207](#) (内核) 添加了有关 Soft-RoCE 驱动程序 `rdma_rxe` 的信息。

#### 0.2-9

2021 年 10 月 7 日星期四, Lenka Špačková ([lspackova@redhat.com](mailto:lspackova@redhat.com))

- 更新了已知问题 [BZ#1942330](#) (动态编程语言、Web 和数据库服务器)。

#### 0.2-8

2021 年 10 月 5 日星期二, Lucie Maňásková ([Imanasko@redhat.com](mailto:Imanasko@redhat.com))

- 添加了已弃用的功能 [BZ#1999620](#) (Shells 和命令行工具)。

#### 0.2-7

2021 年 8 月 19 日星期四, Lucie Maňásková ([Imanasko@redhat.com](mailto:Imanasko@redhat.com))

- 向分发一章中添加了 [使用 YUM/DNF 的软件包管理](#)。
- 更新了 [BZ#1708456](#) (内核) 的文本。

#### 0.2-6

2021 年 7 月 9 日星期五, Lucie Maňásková ([Imanasko@redhat.com](mailto:Imanasko@redhat.com))

- 更新了 [JIRA : RHELPLAN-34199](#) (安全性) 的文本。

#### 0.2-5

2021 年 6 月 23 日星期三, Lucie Maňásková ([Imanasko@redhat.com](mailto:Imanasko@redhat.com))

- 添加了有关删除 [BZ#1922488](#) (桌面) 中的 AlternateTab 的信息。

#### 0.2-4

2021 年 5 月 21 日星期五, Lenka Špačková ([lspackova@redhat.com](mailto:lspackova@redhat.com))

- 更新了 [Overview](#) 中有关操作系统转换的信息。

#### 0.2-3

2021 年 5 月 20 日星期二, Lenka Špačková ([lspackova@redhat.com](mailto:lspackova@redhat.com))

- 添加了对已知问题 [BZ#1942330](#) (动态编程语言、Web 和数据库服务器) 的临时解决方案。

#### 0.2-2

2021 年 5 月 14 日星期五, Lucie Maňásková ([Imanasko@redhat.com](mailto:Imanasko@redhat.com))

- 添加了一个关于 .NET 5 支持 (编译器和开发工具) 的新特性 [BZ#1944677](#)。
- 添加了一个新特性 `xfer:BZ-1959289[BZ#1959289]` (RHEL 系统角色)。
- 更新了有关 [BZ#1820670](#) (网络) 和 [BZ#1780124](#) (内核) 中 `xdp-tools` 软件包的信息。

#### 0.2-1

2021 年 4 月 19 日 星期一, Lenka Špačková ([lspackova@redhat.com](mailto:lspackova@redhat.com))

- 添加了一个已知问题 [BZ#1942330](#) (动态编程语言、Web 和数据库服务器)。

#### 0.2-0

2021 年 4 月 13 日 星期二, Lenka Špačková ([lspackova@redhat.com](mailto:lspackova@redhat.com))

- 添加了一个已知问题 (安装程序和镜像创建)。

#### 0.1-9

2021 年 4 月 6 日 星期二, Lenka Špačková ([lspackova@redhat.com](mailto:lspackova@redhat.com))

- 改进了支持的构架列表。

#### 0.1-8

2021 年 3 月 31 日 星期三, Lenka Špačková ([lspackova@redhat.com](mailto:lspackova@redhat.com))

- 使用支持的 **Convert2RHEL** 工具更新了有关操作系统转换的信息。

#### 0.1-7

2021 年 3 月 29 日 星期一, Lucie Maňásková ([lmanasko@redhat.com](mailto:lmanasko@redhat.com))

- 更新了新特性部分(内核)。

#### 0.1-6

2021 年 2 月 25 日 星期四, Lenka Špačková ([lspackova@redhat.com](mailto:lspackova@redhat.com))

- 修复了 CentOS Linux 名称。

#### 0-1-5

2021 年 2 月 23 日 星期二, Lucie Maňásková ([lmanasko@redhat.com](mailto:lmanasko@redhat.com))

- 添加了一个已知问题 (身份管理)。
- 在 RHEL 8.3.1 部分中添加了一个有关 **podman** 工具 rebase 的备注。

#### 0-1-4

2021 年 2 月 18 日 星期四, Jaroslav Klech ([jklech@redhat.com](mailto:jklech@redhat.com))

- 添加了一个已知问题(内核)。
- 修复了一个增强的链接(内核)。

#### 0-1-3

2021 年 2 月 16 日 星期二, Lenka Špačková ([lspackova@redhat.com](mailto:lspackova@redhat.com))

- 发布了 Red Hat Enterprise Linux 8.3.1 发行注记。
- 通过 [RHBA-2021:0569](#) 公告的发布, 更新了概述中的原位升级部分。

#### 0-1-2

2021 年 2 月 12 日 星期五, Lucie Maňásková ([lmanasko@redhat.com](mailto:lmanasko@redhat.com))



- 增加了两个已知问题（安全、安装程序）。

#### 0-1-1

2021 年 2 月 10 日星期三, Lucie Maňásková ([Imanasko@redhat.com](mailto:Imanasko@redhat.com))

- 增加了一个已知问题（虚拟化）。

#### 0-1-0

2021 年 2 月 3 日星期三, Lenka Špačková ([lspackova@redhat.com](mailto:lspackova@redhat.com))

- 增加了关于内核命令行中 **ip** 参数（网络）下的网络配置整合的备注。
- 将 **mercurial** 添加到已弃用的软件包中。
- 增加了与 Witherspoon 主机（虚拟化）有关的已知问题。

#### 0-0-9

2021 年 1 月 29 日星期五, Lucie Maňásková ([Imanasko@redhat.com](mailto:Imanasko@redhat.com))

- 增加了新的 bug 修复描述(安全)。
- 增加了有关 **mailman** 软件包（软件管理）弃用的备注。
- 更新了新特性部分（安全、身份管理）。
- 增加了有关 **systemd-resolved** 服务的技术预览的备注。
- 其他次要更新。

#### 0.0-8

2020 年 12 月 14 日星期一, Lucie Maňásková ([Imanasko@redhat.com](mailto:Imanasko@redhat.com))

- 更新了已知问题部分和 bug 修复部分。

#### 0.0-7

2020 年 11 月 27 日星期五, Lucie Maňásková ([Imanasko@redhat.com](mailto:Imanasko@redhat.com))

- 增加了对 **fapolicyd** (安全)问题的 bug 修复。
- bug 修复部分的更多更新。
- 增加了有关基于 Podman varlink 的 REST API V1（容器）弃用的备注。
- 更新了新特性部分。
- 增加了有关将蓝图从 **lorax-composer** 后端复制到新 **osbuild-composer** 后端(Image Builder)的新的已知问题。

#### 0.0-6

2020 年 11 月 20 日星期五, Lucie Maňásková ([Imanasko@redhat.com](mailto:Imanasko@redhat.com))

- 增加了 OpenSCAP bug 修复描述（安全）。
- 更新了新特性部分（软件管理）。

#### 0.0-5

2020 年 11 月 18 日星期三, Lenka Špačková ([lspackova@redhat.com](mailto:lspackova@redhat.com))

- 添加了有关从 Oracle Linux 或 CentOS Linux 转换到 RHEL 的信息(概述)。

#### 0.0-4

2020 年 11 月 12 日星期四, Lenka Špačková ([lspackova@redhat.com](mailto:lspackova@redhat.com))

- 添加了与 [RHEA-2020:5101](#) 公告一起发布的有关 **Node.js 14.15.0** 的信息。

#### 0.0-3

2020 年 11 月 11 日星期三, Lucie Maňásková ([Imanasko@redhat.com](mailto:Imanasko@redhat.com))

- 向新特性中添加了有关 Omni-Path 架构(OPA)主机软件支持的描述。

#### 0.0-2

2020 年 11 月 9 日星期一, Lenka Špačková ([lspackova@redhat.com](mailto:lspackova@redhat.com))

- 添加了将 Intel Tiger Lake 图形作为技术预览（图形基础架构）。

#### 0.0-1

Wed Nov 04 2020, Lucie Maňásková([Imanasko@redhat.com](mailto:Imanasko@redhat.com))

- 发布了 Red Hat Enterprise Linux 8.3 发行注记。

#### 0.0-0

Tue Jul 28 2020, Lucie Maňásková([Imanasko@redhat.com](mailto:Imanasko@redhat.com))

- 发布了 Red Hat Enterprise Linux 8.3 Beta 发行注记。