Red Hat Enterprise Linux 8

8.9 リリースノート

Red Hat Enterprise Linux 8.9 のリリースノート

Last Updated: 2024-07-02

Red Hat Enterprise Linux 8 8.9 リリースノート

Red Hat Enterprise Linux 8.9 のリリースノート

法律上の通知

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 ® is the registered trademark of Linus Torvalds in the United States and other countries.

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

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

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

Node.js ® 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 ® 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.

概要

このリリースノートでは、Red Hat Enterprise Linux 8.9 での改良点および実装された追加機能の概要、このリリースにおける既知の問題などを説明します。また、重要なバグ修正、テクニカルプレビュー、非推奨機能などの詳細も説明します。 Red Hat Enterprise Linux のインストールは、Installation を参照してください。

目次

RED HAT ドキュメントへのフィードバック (英語のみ) 5

第1章 概要 6
1.1. RHEL 8.9 における主な変更点 6
1.2. インプレースアップグレードおよび OS 移行 7
1.3. RED HAT CUSTOMER PORTAL LABS 8
1.4. 関連情報 9

第2章 アーキテクチャー 10

第3章 RHEL 8 のコンテンツの配布 11
3.1. インストール 11
3.2. リポジトリー 11
3.3. アプリケーションストリーム 12
3.4. YUM/DNF を使用したパッケージ管理 12

第4章 新機能 13
4.1. インストーラーおよびイメージの作成 13
4.2. セキュリティー 13
4.3. インフラストラクチャーサービス 17
4.4. ネットワーク 18
4.5. カーネル 20
4.6. ファイルシステムおよびストレージ 21
4.7. 高可用性およびクラスター 21
4.8. 動的プログラミング言語、WEB サーバー、およびデータベースサーバー 22
4.9. コンパイラーおよび開発ツール 24
4.10. IDENTITY MANAGEMENT 41
4.11. グラフィックインフラストラクチャー 44
4.12. WEB コンソール 44
4.13. RED HAT ENTERPRISE LINUX システムロール 45
4.14. クラウド環境の RHEL 49
4.15. サポート性 50
4.16. コンテナー 51

第5章 外部カーネルパラメーターへの重要な変更 54
新しいカーネルパラメーター 54
更新されたカーネルパラメーター 54

第6章 デバイスドライバー 57
6.1. 新しいドライバー 57
6.2. 更新されたドライバー 57

第7章 利用可能な BPF 機能 59

第8章 バグ修正 73
8.1. インストーラーおよびイメージの作成 73
8.2. セキュリティー 73
8.3. ソフトウェア管理 78
8.4. シェルおよびコマンドラインツール 78
8.5. ネットワーク 79
8.6. ブートローダー 79
8.7. ファイルシステムおよびストレージ 80
8.8. 高可用性およびクラスター 80

8.9. コンパイラーおよび開発ツール 82
8.10. IDENTITY MANAGEMENT 83
8.11. グラフィックインフラストラクチャー 85
8.12. WEB コンソール 85
8.13. RED HAT ENTERPRISE LINUX システムロール 85
8.14. 仮想化 89

第9章 テクノロジープレビュー 90
9.1. インフラストラクチャーサービス 90
9.2. ネットワーク 90
9.3. カーネル 91
9.4. ファイルシステムおよびストレージ 93
9.5. 高可用性およびクラスター 95
9.6. IDENTITY MANAGEMENT 96
9.7. デスクトップ 98
9.8. グラフィックインフラストラクチャー 99
9.9. 仮想化 99
9.10. クラウド環境の RHEL 101
9.11. コンテナー 101

第10章 非推奨になった機能 103
10.1. インストーラーおよびイメージの作成 103
10.2. セキュリティー 104
10.3. サブスクリプションの管理 106
10.4. ソフトウェア管理 106
10.5. シェルおよびコマンドラインツール 106
10.6. ネットワーク 108
10.7. カーネル 109
10.8. ブートローダー 110
10.9. ファイルシステムおよびストレージ 110
10.10. 高可用性およびクラスター 112
10.11. 動的プログラミング言語、WEB サーバー、およびデータベースサーバー 112
10.12. コンパイラーおよび開発ツール 113
10.13. IDENTITY MANAGEMENT 113
10.14. デスクトップ 116
10.15. グラフィックインフラストラクチャー 117
10.16. WEB コンソール 117
10.17. RED HAT ENTERPRISE LINUX システムロール 118
10.18. 仮想化 119
10.19. コンテナー 120
10.20. 非推奨のパッケージ 122
10.21. 非推奨のデバイスおよび非保守のデバイス 159

第11章 既知の問題 163
11.1. インストーラーおよびイメージの作成 163
11.2. セキュリティー 165
11.3. サブスクリプションの管理 172
11.4. ソフトウェア管理 173
11.5. シェルおよびコマンドラインツール 173
11.6. インフラストラクチャーサービス 174
11.7. ネットワーク 175
11.8. カーネル 176
11.9. ファイルシステムおよびストレージ 182
11.10. 動的プログラミング言語、WEB サーバー、およびデータベースサーバー 183

11.11. IDENTITY MANAGEMENT 185
11.12. デスクトップ 187
11.13. グラフィックインフラストラクチャー 188
11.14. RED HAT ENTERPRISE LINUX システムロール 190
11.15. 仮想化 190
11.16. クラウド環境の RHEL 195
11.17. サポート性 197
11.18. コンテナー 198

第12章 国際化 **199**
12.1. RED HAT ENTERPRISE LINUX 8 の多言語 199
12.2. RHEL 8 における国際化の主な変更点 199

付録A コンポーネント別のチケットリスト **201**

付録B 改訂履歴 **209**

RED HAT ドキュメントへのフィードバック (英語のみ)

Red Hat ドキュメントに関するご意見やご感想をお寄せください。また、改善点があればお知らせください。

Jira からのフィードバック送信 (アカウントが必要)

1. Jira の Web サイトにログインします。
2. 上部のナビゲーションバーで **Create** をクリックします。
3. **Summary** フィールドにわかりやすいタイトルを入力します。
4. **Description** フィールドに、ドキュメントの改善に関するご意見を記入してください。ドキュメントの該当部分へのリンクも追加してください。
5. ダイアログの下部にある **Create** をクリックします。

第1章 概要

1.1. RHEL 8.9 における主な変更点

インストーラーおよびイメージの作成
Image Builder の主なハイライト:

- AWS EC2 AMD または Intel 64 ビットアーキテクチャー AMI イメージが強化され、従来の BIOS ブートに加えて UEFI ブートもサポートされます。

詳細は、新機能 - インストーラーとイメージの作成 を参照してください

セキュリティー
セキュリティー関連の主なハイライト:

- **OpenSCAP** がバージョン 1.3.8 にリベースされました。
- **ANSSI-BP-028** SCAP セキュリティープロファイルがバージョン 2.0 に更新される
- **SCAP セキュリティーガイド** に、より一貫性のあるインタラクティブユーザー設定を提供する改良されたルールが含まれるようになり、DISA STIG プロファイルは **audit_rules_login_events_faillock** をサポートします。

詳細は、新機能 - セキュリティー を参照してください。

動的プログラミング言語、Web サーバー、およびデータベースサーバー
Node.js 20 が新しいモジュールストリームとして利用できるようになりました。

詳細は、新機能 - 動的プログラミング言語、Web サーバー、およびデータベースサーバー を参照してください。

コンパイラーおよび開発ツール
パフォーマンスツールとデバッガーの更新
RHEL 8.9 では、以下のパフォーマンスツールおよびデバッガーが更新されました。

- **Valgrind 3.21**
- **SystemTap 4.9**
- **elfutils 0.189**

更新されたパフォーマンスモニタリングツール
RHEL 8.9 では、以下のパフォーマンス監視ツールが更新されました。

- **Grafana 9.2.10**
- **grafana-pcp 5.1.1**

更新されたコンパイラーツールセット
次のコンパイラーツールセットが RHEL 8.9 で更新されました。

- **GCC Toolset 13** (新規)
- **LLVM Toolset 16.0.6**
- **Rust Toolset 1.71.1**

- Go Toolset 1.20.10

詳しくは 新機能 - コンパイラーおよび開発ツール をご覧ください。

RHEL 8 の Java 実装
RHEL 8 AppStream リポジトリーには、以下が含まれます。

- **java-21-openjdk** パッケージ。OpenJDK 21 Java Runtime Environment および OpenJDK 21 Java Software Development Kit を提供します。
- **java-17-openjdk** パッケージ。OpenJDK 17 Java Runtime Environment および OpenJDK 17 Java Software Development Kit を提供します。
- **java-11-openjdk** パッケージ。OpenJDK 11 Java Runtime Environment および OpenJDK 11 Java Software Development Kit を提供します。
- **java-1.8.0-openjdk** パッケージ。OpenJDK 8 Java Runtime Environment および OpenJDK 8 Java Software Development Kit を提供します。

Red Hat build of OpenJDK パッケージは、ポータブル Linux リリースと RHEL 8.9 以降のリリース間で単一のバイナリーセットを共有します。この更新により、ソース RPM から RHEL 上で OpenJDK パッケージを再構築するプロセスが変更されました。新しい再構築プロセスの詳細は、Red Hat build of OpenJDK の SRPM パッケージで利用可能な **README.md** ファイルを参照してください。これは、**/usr/share/doc** ツリーの下にある **java-*-openjdk-headless** パッケージによってもインストールされます。

詳細は、OpenJDK のドキュメント を参照してください。

1.2. インプレースアップグレードおよび OS 移行

RHEL 7 から RHEL 8 へのインプレースアップグレード
現在、考えられるインプレースアップグレードパスは以下のとおりです。

- 64 ビット Intel、IBM POWER 8 (little endian)、IBM Z アーキテクチャーでの RHEL 7.9 から RHEL 8.6、RHEL 8.8、および RHEL 8.9 へのアップグレード。
- 64 ビット Intel アーキテクチャーの SAP HANA 搭載システム上における、RHEL 7.9 から RHEL 8.6 および RHEL 8.8 へのアップグレード。

詳細は、Supported in-place upgrade paths for Red Hat Enterprise Linux を参照してください。

インプレースアップグレードの実行方法は、RHEL 7 から RHEL 8 へのアップグレード を参照してください。

SAP 環境があるシステムでインプレースアップグレードを実行する手順については、How to in-place upgrade SAP environments from RHEL 7 to RHEL 8 を参照してください。

主な機能拡張は、次のとおりです。

- **ftype=0** でフォーマットされた XFS ファイルシステムを備えたシステムで、ディスク容量の要件が大幅に軽減されました。
- アップグレードの目的でアップグレードプロセス中に作成されるディスクイメージのサイズが動的になりました。**LEAPP_OVL_SIZE** 環境変数が不要になりました。
- 既存のディスクパーティションに必要な空き領域の計算に関する問題が修正されました。システムの再起動が必要になる前に、不足している空きディスク領域が正しく検出されるようにな

り、アップグレード RPM トランザクションを続行するのに十分な空き領域がないファイルシステムがレポートに正しく表示されるようになりました。

- カスタム Leapp アクターを使用して、インプレースアップグレードプロセス中にサードパーティードライバーを管理できるようになりました。
- アップグレード前レポートとアップグレードレポートの概要が端末に印刷されるようになりました。
- Red Hat OpenStack Platform の RHEL Real Time および RHEL Real Time for Network Functions Virtualization (NFV) のアップグレードがサポートされるようになりました。

RHEL 6 から RHEL 8 へのインプレースアップグレード
RHEL 6 から RHEL 8 へのインプレースアップグレードを直接実行することはできません。ただし、RHEL 6 から RHEL 7 へのインプレースアップグレードを実行してから、RHEL 8 への 2 回目のインプレースアップグレードを実行することはできます。詳細は、RHEL 6 から RHEL 7 へのアップグレードを参照してください。

RHEL 8 から RHEL 9 へのインプレースアップグレード
Leapp ユーティリティーを使用して RHEL 8 から RHEL 9 へのインプレースアップグレードを行う方法は、RHEL 8 から RHEL 9 へのアップグレード を参照してください。RHEL 8 と RHEL 9 の主な相違点は、RHEL 9 の導入における検討事項 を参照してください。

別の Linux ディストリビューションから RHEL への移行
Alma Linux 8、CentOS Linux 8、Oracle Linux 8、または Rocky Linux 8 を使用している場合は、Red Hat がサポートする **Convert2RHEL** ユーティリティーを使用してオペレーティングシステムを RHEL 8 に変換できます。詳細は、RPM ベースの Linux ディストリビューションから RHEL への変換 を参照してください。

CentOS Linux または Oracle Linux の旧バージョン (バージョン 6 または 7) を使用している場合は、お使いのオペレーティングシステムを RHEL に移行してから、RHEL 8 へのインプレースアップグレードを実行できます。CentOS Linux 6 および Oracle Linux 6 変換は、サポート対象外の **Convert2RHEL** ユーティリティーを使用することに注意してください。サポートされていない変換の詳細については、How to perform an unsupported conversion from a RHEL-derived Linux distribution to RHEL を参照してください。

Red Hat が他の Linux ディストリビューションから RHEL への移行は、Convert2RHEL サポートポリシー を参照してください。

1.3. RED HAT CUSTOMER PORTAL LABS

Red Hat Customer Portal Labsは、カスタマーポータルのセクションにあるツールセットで、https://access.redhat.com/labs/ から入手できます。Red Hat Customer Portal Labs のアプリケーションは、パフォーマンスの向上、問題の迅速なトラブルシューティング、セキュリティー問題の特定、複雑なアプリケーションの迅速なデプロイメントおよび設定に役立ちます。最も一般的なアプリケーションには、以下のものがあります。

- Registration Assistant
- Product Life Cycle Checker
- Kickstart Generator
- Kickstart Converter
- Red Hat Enterprise Linux Upgrade Helper

- Red Hat Satellite Upgrade Helper
- Red Hat Code Browser
- JVM Options Configuration Tool
- Red Hat CVE Checker
- Red Hat Product Certificates
- Load Balancer Configuration Tool
- Yum Repository Configuration Helper
- Red Hat Memory Analyzer
- Kernel Oops Analyzer
- Red Hat Product Errata Advisory Checker

1.4. 関連情報

- 他のバージョンと比較した Red Hat Enterprise Linux 8.0 の **機能および制限** は、Red Hat ナレッジベースの記事 Red Hat Enterprise Linux technology capabilities and limits を参照してください。
- Red Hat Enterprise Linux の **ライフサイクル** に関する情報は Red Hat Enterprise Linux のライフサイクル を参照してください。
- RHEL 8 の **パッケージリスト** は、パッケージマニフェスト を参照してください。
- 削除された機能を含む主な**RHEL 7 と RHEL 8 の相違点**は、RHEL 8 の導入における考慮事項 で説明されています。
- **RHEL 7 から RHEL 8 へのインプレースアップグレード**を実行する方法は、Upgrading from RHEL 7 to RHEL 8 を参照してください。
- すべての RHEL サブスクリプションで、既知の技術問題の特定、検証、および解決をプロアクティブに行う **Red Hat Insights** サービスが利用できるようになりました。Red Hat Insights クライアントをインストールし、システムをサービスに登録する方法は、Red Hat Insights を使い始める ページを参照してください。

注記

リリースノートには、元の追跡チケットにアクセスするためのリンクが含まれています。プライベートチケットにはリンクがなく、代わりにこの脚注が表示されます。[1]

[1] リリースノートには、元の追跡チケットにアクセスするためのリンクが含まれています。プライベートチケットにはリンクがなく、代わりにこの脚注が表示されます。

第2章 アーキテクチャー

Red Hat Enterprise Linux 8.9 には、カーネルバージョン 4.18.0-513.5.1 が同梱されており、以下のアーキテクチャーに対応します。

- AMD アーキテクチャーおよび Intel 64 ビットアーキテクチャー
- 64 ビット ARM アーキテクチャー
- IBM Power Systems (リトルエンディアン)
- 64 ビット IBM Z

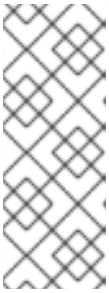
各アーキテクチャーに適切なサブスクリプションを購入してください。詳細は Get Started with Red Hat Enterprise Linux - additional architectures を参照してください。利用可能なサブスクリプションのリストは、カスタマーポータルの サブスクリプションの使用状況 を参照してください。

第3章 RHEL 8 のコンテンツの配布

3.1. インストール

Red Hat Enterprise Linux 8 は、ISO イメージを使用してインストールします。AMD64、Intel 64 ビット、64 ビット ARM、IBM Power Systems、IBM Z アーキテクチャーで、以下の 2 種類のインストールメディアが利用できます。

- Binary DVD ISO - BaseOS リポジトリーおよび AppStream リポジトリーが含まれ、リポジトリーを追加しなくてもインストールを完了できる完全インストールイメージです。



注記

インストール用 ISO イメージのサイズは複数 GB であるため、光学メディア形式には適合しない場合があります。インストール ISO イメージを使用して起動可能なインストールメディアを作成する場合は、USB キーまたは USB ハードドライブを使用することが推奨されます。Image Builder ツールを使用すれば、RHEL イメージをカスタマイズできます。Image Builder の詳細は **RHEL システムイメージのカスタマイズの作成** を参照してください。

- Boot ISO - インストールプログラムを起動するのに使用する最小限の ISO ブートイメージです。このオプションでは、ソフトウェアパッケージをインストールするのに、BaseOS リポジトリーおよび AppStream リポジトリーにアクセスする必要があります。リポジトリーは、Binary DVD ISO イメージに含まれます。

ISO イメージのダウンロード、インストールメディアの作成、および RHEL インストールの完了の手順については 標準的な RHEL 8 インストールの実行 ドキュメントを参照してください。自動化したキックスタートインストールなどの高度なトピックは 高度な RHEL 8 インストールの実行 を参照してください。

3.2. リポジトリー

Red Hat Enterprise Linux 8 は、2 つのメインリポジトリーで配布されています。

- BaseOS
- AppStream

基本的な RHEL インストールにはどちらのリポジトリーも必要で、すべての RHEL サブスクリプションで利用できます。

BaseOS リポジトリーのコンテンツは、すべてのインストールのベースとなる、基本的な OS 機能のコアセットを提供します。このコンテンツは RPM 形式で提供されており、RHEL の以前のリリースと同様のサポート条件が適用されます。BaseOS から配布されるパッケージのリストは パッケージマニフェスト を参照してください。

アプリケーションストリーム (AppStream) リポジトリーのコンテンツには、さまざまなワークロードとユースケースに対応するために、ユーザー空間アプリケーション、ランタイム言語、およびデータベースが含まれています。Application Streams は、**モジュール** と呼ばれる RPM 形式への拡張、または Software Collections として通常の RPM 形式で利用できます。AppStream で利用可能なパッケージのリストは、パッケージマニフェスト を参照してください。

また、CodeReady Linux Builder リポジトリーは、すべての RHEL サブスクリプションで利用できます。このリポジトリーは、開発者向けの追加パッケージを提供します。CodeReady Linux Builder リポジトリーに含まれるパッケージには対応しません。

RHEL 8 リポジトリーの詳細は パッケージマニフェスト を参照してください。

3.3. アプリケーションストリーム

Red Hat Enterprise Linux 8 では、アプリケーションストリームの概念が導入されました。ユーザー空間コンポーネントのバージョンが複数配信され、オペレーティングシステムのコアパッケージよりも頻繁に更新されるようになりました。これにより、プラットフォームや特定デプロイメントの基本的な安定性に影響を及ぼすことなく、Red Hat Enterprise Linux をカスタマイズできる柔軟性が向上しました。

アプリケーションストリームとして使用できるコンポーネントは、モジュールまたは RPM パッケージとしてパッケージ化され、RHEL 8 の AppStream リポジトリーを介して配信されます。各 Application Stream コンポーネントには、RHEL 8 と同じか、より短いライフサイクルが指定されています。詳細は Red Hat Enterprise Linux のライフサイクル を参照してください。

モジュールは、論理ユニット (アプリケーション、言語スタック、データベース、またはツールセット) を表すパッケージの集まりです。これらのパッケージはまとめてビルドされ、テストされ、そしてリリースされます。

モジュールストリームは、アプリケーションストリームコンポーネントのバージョンを表します。たとえば、**postgresql:10** のデフォルトのストリーム以外に、**postgresql** モジュールでは、PostgreSQL データベースサーバーの複数のストリーム (バージョン) を利用できます。システムにインストールできるモジュールストリームは 1 つだけです。複数のコンテナーで異なるバージョンを使用できます。

詳細なモジュールコマンドは ユーザー空間コンポーネントのインストール、管理、および削除 を参照してください。AppStream で利用可能なモジュールのリストは、Package manifest を参照してください。

3.4. YUM/DNF を使用したパッケージ管理

Red Hat Enterprise Linux 8 へのソフトウェアのインストールは、**DNF** テクノロジーをベースとした **YUM** ツールにより行われます。以前のメジャーバージョンの RHEL との一貫性を保つために、 **yum** の用語の使用が意図的に準拠しています。ただし、**yum** の代わりに **dnf** を呼び出すと、**yum** は互換性のために **dnf** のエイリアスであるため、コマンドが期待どおりに動作します。

詳細は、以下のドキュメントを参照してください。

- ユーザー空間コンポーネントのインストール、管理、および削除
- RHEL 8 の導入における検討事項

第4章 新機能

ここでは、Red Hat Enterprise Linux 8.9 に追加された新機能および主要な機能拡張を説明します。

4.1. インストーラーおよびイメージの作成

AWS EC2 イメージのレガシーブートと UEFI ブートの両方をサポート

以前は、RHEL Image Builder は、レガシーブートタイプのみをサポートする EC2 AMD または Intel 64 ビットアーキテクチャーの AMI イメージを作成していました。その結果、セキュアブートなど、UEFI ブートを必要とする特定の AWS 機能を利用できませんでした。この機能拡張により、AWS EC2 AMD または Intel 64 ビットアーキテクチャーの AMI イメージが拡張され、レガシー BIOS ブートに加えて UEFI ブートもサポートされるようになりました。その結果、UEFI でイメージをブートする必要がある AWS の機能を利用できるようになりました。

Jira:RHELDOCS-16339[1]

キックスタートファイルまたはカーネルドライバーをロードするための待機時間を追加する新しいブートオプション inst.wait_for_disks=

場合によっては、ブートプロセス中に **OEMDRV** ラベルが付いたデバイスからキックスタートファイルまたはカーネルドライバーをロードするのに数秒かかることがあります。待機時間を調整するために、新しいブートオプション **inst.wait_for_disks=** を使用できるようになりました。このオプションを使用すると、インストール前に待機する秒数を指定できます。デフォルト時間は **5** 秒に設定されていますが、**0** 秒を使用して遅延を最小限に抑えることができます。このオプションの詳細は、ストレージブートオプション を参照してください。

Bugzilla:1770969

DNS 処理を制御するための新しい network キックスタートオプション

次の新しいオプションを指定した **network** キックスタートコマンドを使用して、DNS 処理を制御できるようになりました。これらの新しいオプションは **--device** オプションと一緒に使用します。

- **--ipv4-dns-search** および **--ipv6-dns-search** オプションを使用すると、DNS 検索ドメインを手動で設定できます。これらのオプションは、それぞれの NetworkManager プロパティーをミラーリングします。次に例を示します。

  ```
  network --device ens3 --ipv4-dns-search domain1.example.com,domain2.example.com
  ```

- **--ipv4-ignore-auto-dns** および **--ipv6-ignore-auto-dns** オプションを使用すると、DHCP からの DNS 設定を無視できます。引数は必要ありません。

Bugzilla:1656662[1]

4.2. セキュリティー

opencryptoki が 3.21.0 にリベース

opencryptoki パッケージはバージョン 3.21.0 にリベースされ、多くの機能拡張とバグ修正が提供されています。最も注目すべき点は、**opencryptoki** が次の機能をサポートするようになったということです。

- ハードウェアセキュリティーモジュール (HSM) マスターキーの同時変更

- 選択したキーを保護されたキーに変換するための **protected-key** オプション
- DH、DSA、汎用シークレットキータイプなどの追加のキータイプ
- EP11 ホストライブラリーバージョン 4
- AES-XTS キーのタイプ
- IBM 固有の Kyber キーのタイプとメカニズム
- 追加の IBM 固有の Dilithium キーラウンド 2 および 3 のバリアント

さらに、**pkcsslotd** スロットマネージャーは root として実行されなくなり、 **opencryptoki** はさらなる強化を提供します。この更新により、次の新しいコマンドのセットも使用できるようになりました。

p11sak set-key-attr
: キーを変更する場合

p11sak copy-key
: キーをコピーする場合

p11sak import-key
: キーをインポートする場合

p11sak export-key
: キーをエクスポートする場合

Bugzilla:2159697[1]

fapolicyd がトラブルシューティング用のルール番号を提供するようになる

この機能拡張では、新しいカーネルおよび Audit コンポーネントにより、**fapolicyd** サービスが拒否を引き起こすルールの番号を **fanotify** API に送信できるようになります。その結果、**fapolicyd** に関連する問題をより正確にトラブルシューティングできます。

Jira:RHEL-628

ANSSI-BP-028 セキュリティープロファイルが、バージョン 2.0 に更新される

SCAP セキュリティーガイド内の以下の French National Agency for the Security of Information Systems (ANSSI) BP-028 プロファイルは、バージョン 2.0 に合わせて更新されました。

- ANSSI-BP-028 Minimal Level
- ANSSI-BP-028 Intermediary Level
- ANSSI-BP-028 Enhanced Level
- ANSSI-BP-028 High Level

Bugzilla:2155789

インタラクティブユーザーの定義の改善

scap-security-guide パッケージのルールが改善され、より一貫性のあるインタラクティブユーザー設定が提供されるようになりました。以前は、一部のルールで、インタラクティブユーザーと非インタラクティブユーザーを識別するために異なるアプローチが使用されていました。この更新により、インタ

ラクティブユーザーの定義が統一されました。UID が 1000 以上のユーザーアカウントは、**nobody** および **nfsnobody** アカウントを除き、またログインシェルとして **/sbin/nologin** を使用するアカウントを除き、インタラクティブユーザーとみなされます。

この変更は次のルールに影響します。

- **accounts_umask_interactive_users**
- **accounts_user_dot_user_ownership**
- **accounts_user_dot_group_ownership**
- **accounts_user_dot_no_world_writable_programs**
- **accounts_user_interactive_home_directory_defined**
- **accounts_user_interactive_home_directory_exists**
- **accounts_users_home_files_groupownership**
- **accounts_users_home_files_ownership**
- **accounts_users_home_files_permissions**
- **file_groupownership_home_directories**
- **file_ownership_home_directories**
- **file_permissions_home_directories**
- **file_permissions_home_dirs**
- **no_forward_files**

Bugzilla:2157877、Bugzilla:2178740

DISA STIG プロファイルが audit_rules_login_events_faillock をサポートするようになりました。

この機能拡張により、STIG ID RHEL-08-030590 を参照する SCAP セキュリティーガイドの **audit_rules_login_events_faillock** ルールが、RHEL 8 の DISA STIG プロファイルに追加されました。このルールは、**/var/log/faillock** ディレクトリーに保存されているログインイベントログを変更しようとする試みを記録するように Audit デーモンが設定されているかどうかを確認します。

Bugzilla:2167999

OpenSCAP が 1.3.8 にリベース

OpenSCAP パッケージがアップストリームバージョン 1.3.8 にリベースされました。このバージョンは、さまざまなバグ修正と機能拡張を提供します。特に、次のとおりです。

- 一部の **systemd** ユニットを無視しないように **systemd** プローブを修正しました
- **shadow** OVAL プローブにオフライン機能を追加しました
- **sysctl** OVAL プローブにオフライン機能を追加しました
- ネットワークファイルシステムのリストに **auristorfs** を追加しました

- **autotailor** ユーティリティーによって生成されたファイルの調整に関する問題の回避策を作成しました。

Bugzilla:2217441

SCAP セキュリティーガイドがバージョン 0.1.69 にリベース

SCAP セキュリティーガイド (SSG) パッケージが、アップストリームバージョン 0.1.69 にリベースされました。このバージョンでは、さまざまな機能拡張とバグ修正が提供されています。特に注目すべきは、2022 年 10 月に National Cryptologic Center of Spain によって発行された CCN-STIC-610A22 ガイドの 3 つのレベルに準拠した RHEL 9 用の 3 つの新しい SCAP プロファイルです。

- CCN Red Hat Enterprise Linux 9 - Basic
- CCN Red Hat Enterprise Linux 9 - Intermediate
- CCN Red Hat Enterprise Linux 9 - Advanced

Bugzilla:2221695

RHEL 8.8 以降から RHEL 9.2 以降への FIPS 対応のインプレースアップグレードがサポートされます。

RHBA-2023:3824 アドバイザリーのリリースにより、FIPS モードが有効な RHEL 8.8 以降のシステムから RHEL 9.2 以降のシステムへのインプレースアップグレードを実行できるようになりました。

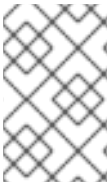
Bugzilla:2097003

crypto-policies permitted_enctypes が FIPS モードでのレプリケーションを破損しなくなる

この更新前は、RHEL 8 で実行されている IdM サーバーは、FIPS モードで RHEL 9 を実行している IdM レプリカに AES-256-HMAC-SHA-1 で暗号化されたサービスチケットを送信していました。その結果、デフォルトの **permitted_enctypes krb5** 設定により、FIPS モードでの RHEL 8 IdM サーバーと RHEL 9 IdM レプリカ間のレプリケーションが破損していました。

この更新により、**allowed_enctypes krb5** 設定オプションの値が、**mac** および **cipher crypto-policy** の値に依存するようになりました。これにより、相互運用可能な暗号化タイプの優先順位付けがデフォルトで可能になります。

この更新の追加結果として、**arcfour-hmac-md5** オプションが **LEGACY:AD-SUPPORT** サブポリシーでのみ使用可能になり、**aes256-cts-hmac-sha1-96** が **FUTURE** ポリシーで使用できなくなりました。



注記

Kerberos を使用する場合は、**/etc/crypto-policies/back-ends/krb5.config** ファイル内の **permitted_enctypes** の値の順序を確認してください。別の順序が必要な場合は、カスタム暗号化サブポリシーを適用します。

Bugzilla:2219912

Audit が FANOTIFY レコードフィールドをサポートするようになる

audit パッケージの今回の更新で、**FANOTIFY** Audit レコードフィールドがサポートされるようになりました。Audit サブシステムは、特に次のような追加情報を **AUDIT_FANOTIFY** レコードに記録するようになりました。

- **fan_type**: **FANOTIFY** イベントのタイプを指定する

- **fan_info**: 追加のコンテキスト情報を指定する
- **sub_trust** と **obj_trust**: イベントに関与するサブジェクトとオブジェクトの信頼レベルを示す

これにより、特定のケースで Audit システムがアクセスを拒否した理由をよりよく理解できます。これは、**fapolicyd** フレームワークなどのツールのポリシーを作成する場合に役立ちます。

Bugzilla:2216666

QEMU ゲストエージェントが限定されたコマンドを実行できるようにする新しい SELinux ブール値

以前は、QEMU ゲストエージェントデーモンプログラムを通じて限定されたコンテキストで実行されるはずのコマンド (**mount** など) が、アクセスベクターキャッシュ (AVC) 拒否で失敗していました。これらのコマンドを実行するには、**guest-agent** が **virt_qemu_ga_unconfined_t** ドメインで実行されている必要があります。

したがって、この更新では、SELinux ポリシーブール値 **virt_qemu_ga_run_unconfined** が追加され、**guest-agent** が以下のいずれかのディレクトリーにある実行可能ファイルに対して **virt_qemu_ga_unconfined_t** に移行できるようになります。

- **/etc/qemu-ga/fsfreeze-hook.d/**
- **/usr/libexec/qemu-ga/fsfreeze-hook.d/**
- **/var/run/qemu-ga/fsfreeze-hook.d/**

さらに、**qemu-ga** デーモンの移行に必要なルールが SELinux ポリシーのブール値に追加されました。

その結果、**virt_qemu_ga_run_unconfined** ブール値を有効にすることで、AVC 拒否なしで QEMU ゲストエージェントを通じて制限されたコマンドを実行できるようになりました。

Bugzilla:2093355

4.3. インフラストラクチャーサービス

Postfix が SRV ルックアップをサポートするようになる

この機能拡張により、Postfix DNS サービスレコード解決 (SRV) を使用して、メールクライアントを自動的に設定し、サーバーの負荷を分散できるようになりました。さらに、Postfix 設定で次の SRV 関連のオプションを使用することで、一時的な DNS の問題や SRV レコードの設定ミスによるメール配信の中断を防ぐことができます。

use_srv_lookup
: DNS SRV レコードを使用して、指定したサービスの検出を有効にできます。

allow_srv_lookup_fallback
: カスケードアプローチを使用してサービスを見つけることができます。

ignore_srv_lookup_error
: SRV レコードが利用できない場合やエラーが発生した場合でも、サービス検出は機能し続けることができます。

Bugzilla:1787010

vsftpd で TLS 1.3 暗号スイートを指定できるようになりました。

この機能拡張により、新しい **ssl_ciphersuites** オプションを使用して、**vsftpd** が使用する暗号スイートを設定できるようになりました。その結果、以前の TLS バージョンとは異なる TLS 1.3 暗号スイートを指定できます。複数の暗号スイートを指定するには、エントリーをコロン (:) で区切ります。

Bugzilla:2069733

Generic LF-to-CRLF ドライバーが cups-filters で利用可能になる

この機能拡張により、CR+LF 文字を含むファイルを受け入れるプリンターで、LF 文字を CR+LF 文字に変換する Generic LF-to-CRLF ドライバーを使用できるようになりました。キャリッジリターン (CR) とラインフィード (LF) は、行の終わりを示す制御文字です。その結果、このドライバーを使用すると、LF 文字で終了するファイルをアプリケーションから CR+LF 文字のみを受け入れるプリンターに送信できます。Generic LF-to-CRLF ドライバーは、RHEL 7 の **text-only** ドライバーの名前が変更されたバージョンです。新しい名前は実際の機能を反映しています。

Bugzilla:2118406[1]

4.4. ネットワーク

iproute がバージョン 6.2.0 にリベース

iproute パッケージはアップストリームバージョン 6.2.0 にアップグレードされ、以前のバージョンに比べて多くの機能拡張とバグ修正が行われました。主な変更点は以下のとおりです。

- 新しい **ip stats** コマンドは、インターフェイス統計を管理および表示します。デフォルトでは、**ip stats show** コマンドは、ブリッジやボンディングを含むすべてのネットワークデバイスの統計情報を表示します。**dev** および **group** オプションを使用して出力をフィルタリングできます。詳細は、**ip-stats(8)** の man ページを参照してください。
- **ss** ユーティリティーは、スレッド情報を表示するための **-T** (**--threads**) オプションを提供するようになりました。これは、**-p** (**--processes**) オプションを拡張したものです。詳細は、**ss(8)** の man ページを参照してください。
- 新しい **bridge fdb flush** コマンドを使用すると、指定されたオプションに一致する特定の forwarding database (fdb) エントリーを削除できます。詳細は、**bridge(8)** の man ページを参照してください。

Jira:RHEL-424[1]

デフォルトの nftables サービス設定のセキュリティー向上

この機能拡張により、**/etc/sysconfig/nftables/nat.nft** ファイル内のデフォルトの **nftables** サービス設定に **do_masquerade** チェーンが追加されます。これにより、CVE-2021-3773 で説明されているポートシャドウ攻撃のリスクが軽減されます。**do_masquerade** チェーンの最初のルールが、適切なパケットを検出し、送信元ポートのランダム化を適用して、ポートシャドウ攻撃のリスクを軽減します。

Bugzilla:2061942

NetworkManager が no-aaaa DNS オプションをサポートするようになりました。

no-aaaa オプションを使用して、スタブリゾルバーによって生成された AAAA クエリーを抑制することにより、マネージドノードで DNS 設定を設定できるようになりました。以前は、**getaddrinfo** などの NSS ベースのインターフェイスによってトリガーされる AAAA ルックアップを含む、スタブリゾルバーによって生成される AAAA クエリーを抑制するオプションはありませんでした。DNS ルックアップのみが影響を受けていました。この機能拡張により、**nmcli** ユーティリティーを使用して IPv6 解決を無効にできるようになりました。**NetworkManager** サービスの再起動後、**no-aaaa** 設定が **/etc/resolv.conf** ファイルに反映され、DNS ルックアップの制御が追加されます。

Bugzilla:2144521

nm-cloud-setup ユーティリティーが IMDSv2 設定をサポートするようになる

ユーザーは、**nm-cloud-setup** ユーティリティーを使用して、Instance Metadata Service Version 2 (IMDSv2)を使用する AWS Red Hat Enterprise Linux EC2 インスタンスを設定できます。EC2 メタデータや新機能への不正アクセスを制限するセキュリティー強化に準拠するには、高度な機能を提供するために AWS と Red Hat のサービスを統合する必要があります。この機能拡張により、**nm-cloud-setup** ユーティリティーは保護された IMDSv2 トークンを使用することで、IMDSv2 トークンを取得して保存し、EC2 環境を検証して、利用可能なインターフェイスと IP 設定に関する情報を取得できるようになります。

Bugzilla:2151987

libnftnl パッケージがバージョン 1.2.2 にリベース

カーネル内 **nf_tables** サブシステムの Netlink API (**libnftnl**) のパッケージがリベースされました。注目すべき変更点と機能拡張は次のとおりです。

- 追加された機能:
  - **udata** 属性のネスト
  - **exthdr** 式を使用した TCP オプションのリセット
  - **sdif** および **sdifname** メタキーワード
  - カーネルとユーザー空間の間でフラグを通信するための、**nftnl_chain** 構造体の新しい属性 **NFTNL_CHAIN_FLAGS** のサポート
  - sets および set 要素に式を追加するための、**nftnl_set** 構造体 nftables セットバックエンドのサポート
  - セット、テーブル、オブジェクト、チェーンへのコメント
  - **nftnl_table** 構造体に **NFTNL_TABLE_OWNER** 属性が追加されました。この属性を設定すると、カーネルが所有者をユーザー空間に伝達できるようになります。
  - フローテーブルデバイスに対する増分更新の準備
  - **typeof** キーワード関連の **nftnl_set udata** 定義
  - **chain** ID 属性
  - ルールから式を削除する関数
  - 新しい **last** 表現
- 改善されたビット単位の式:
  - 新しく追加された **op** 属性と **data** 属性
  - 左右のシフト
  - 他の式のデバッグ出力と整合
- 改善されたソケット式:
  - **wildcard** 属性を追加

  - cgroups v2 のサポート
- デバッグ出力の改善:
  - **key_end** データレジスターを set 要素に追加
  - **masq** 式と nat 式から未使用のレジスターを削除
  - 判定マップ要素に適用された修正
  - 削除された XML フォーマットから残存物を削除
  - 内部ヘッダーのペイロードオフセットのサポート

Bugzilla:2211096

4.5. カーネル

RHEL 8.9 のカーネルバージョン

Red Hat Enterprise Linux 8.9 は、カーネルバージョン 4.18.0-513.5.1 で配布されます。

Bugzilla:2232558

RHEL カーネルが AutoIBRS をサポートするようになる

Automatic Indirect Branch Restricted Speculation (AutoIBRS) は、AMD EPYC 9004 Genoa プロセッサーファミリーおよびそれ以降の CPU バージョンによって提供される機能です。AutoIBRS は Spectre v2 CPU の脆弱性に対するデフォルトの軽減策であり、パフォーマンスを向上させ、スケーラビリティーを向上させます。

Bugzilla:1989283[1]

Intel® QAT カーネルドライバーがアップストリームバージョン 6.2 にリベース

Intel® Quick Assist Technology (QAT) は、アップストリームバージョン 6.2 にリベースされました。Intel® QAT には、対称および非対称暗号化、圧縮パフォーマンス、その他の CPU を集中的に使用するタスク用に最適化されたアクセラレーターが含まれています。

リベースには多くのバグ修正と機能拡張が含まれています。最も注目すべき機能拡張は、QAT GEN4 の次のハードウェアアクセラレータデバイスのサポートが利用可能になったことです。

- Intel Quick Assist Technology 401xx デバイス
- Intel Quick Assist Technology 402xx デバイス

Bugzilla:2144529[1]

makedumpfile がバージョン 1.7.2 にリベースされました。

makedumpfile ツールが、バージョン 1.7.2 にリベースされました。これは、ページを圧縮するか、不要なメモリーページを除外することでクラッシュダンプファイルを小さくするツールです。リベースには多くのバグ修正と機能拡張が含まれています。

最も注目すべき変更点は、AMD および Intel 64 ビットアーキテクチャー上のスタンドアロンダンプ (**sadump**) メカニズムに 5 レベルのページングモードが追加されたことです。5 レベルのページングモードは、プロセッサーのリニアアドレスの幅を拡張し、アプリケーションがより大量のメモリーにア

クセスできるようにします。5 レベルのページングにより、仮想アドレスのサイズが 48 ビットから 57 ビットに拡張され、物理アドレスのサイズが 46 ビットから 52 ビットに拡張されます。

Bugzilla:2173791

4.6. ファイルシステムおよびストレージ

GFS2 ファイルシステム作成時の UUID 指定のサポート

mkfs.gfs2 コマンドは、新しい **-U** オプションをサポートするようになりました。これにより、作成するファイルシステムのファイルシステム UUID を指定できるようになります。このオプションを省略した場合、ファイルシステムの UUID はランダムに生成されます。

Bugzilla:2180782

fuse3 では、umount をトリガーせずにディレクトリーエントリーを無効にできるようになる

この更新により、新しいメカニズムが **fuse3** パッケージに追加されました。これにより、エントリーに存在するマウントの **umount** を自動的にトリガーすることなく、ディレクトリーエントリーを無効にすることができます。

Bugzilla:2171095[1]

4.7. 高可用性およびクラスター

Pacemaker のスケジューラーが、必須のコロケーション制約をすべて満たしてから、任意のコロケーション制約を満たすように変更されました。

以前は、コロケーション制約は、必須であるか任意であるかに関係なく、1 つずつ考慮されていました。そのため、ノードの割り当てが可能であっても、特定のリソースを実行できない可能性がありました。Pacemaker のスケジューラーは、任意のコロケーション制約を満たす前に、グループメンバー間の暗黙的な制約を含む、すべての必須のコロケーション制約を満たすことを試みるようになりました。その結果、任意と必須のコロケーション制約が混在するリソースを実行できる可能性が高くなりました。

Bugzilla:1876173

IPaddr2 および IPsrcaddr クラスターリソースエージェントがポリシーベースのルーティングをサポートするようになる

IPaddr2 および **IPsrcaddr** クラスターリソースエージェントは、ポリシーベースのルーティングをサポートするようになりました。これにより、複雑なルーティングシナリオを設定できるようになります。ポリシーベースのルーティングでは、リソースエージェントの **table** パラメーターを設定する必要があります。

Bugzilla:2040110

Filesystem リソースエージェントが EFS ファイルシステムタイプをサポートするようになる

ocf:heartbeat:Filesystem クラスターリソースエージェントは、Amazon Elastic File System (EFS) をサポートするようになりました。**Filesystem** リソースを設定するときに **fstype=efs** を指定できるようになりました。

Bugzilla:2049319

alert_snmp.sh.sample アラートエージェントが SNMPv3 をサポートするようになりました。

alert_snmp.sh.sample アラートエージェント (Pacemaker に付属のサンプルアラートエージェント)

は、SNMPv2 だけでなく SNMPv3 プロトコルもサポートするようになりました。この更新により、**alert_snmp.sh.sample** エージェントを変更せずにコピーして、Pacemaker アラートで SNMPv3 を使用できるようになります。

Bugzilla:2160206

Pacemaker アラートを無効にする新しい enabled アラートメタオプション

Pacemaker アラートとアラート受信者は、**enabled** メタオプションをサポートするようになりました。

- アラートに対して **enabled** メタオプションを **false** に設定すると、アラートが無効になります。
- アラートに対して **enabled** メタオプションを **true** に設定し、特定の受信者に対して **false** に設定すると、その受信者のアラートが無効になります。

enabled メタオプションのデフォルト値は **true** です。このオプションを使用すると、計画されたメンテナンスなどの理由でアラートを一時的に無効にすることができます。

Bugzilla:2078611

Pacemaker Remote ノードが短時間の接続停止の後でも一時的なノード属性を保持するようになりました。

以前は、Pacemaker Remote 接続が失われると、Pacemaker は常に一時ノード属性をパージしていました。接続がすぐに回復でき、その間にリモートデーモンが再起動されなかった場合、これは不要でした。Pacemaker Remote ノードは、回復可能な短時間の接続停止の後でも一時的なノード属性を保持するようになりました。

Bugzilla:2030869

pcs property コマンドの機能拡張

pcs property コマンドは、次の機能拡張をサポートするようになりました。

- **pcs property config --output-format=** オプション
  - **--output-format=cmd** を指定すると、現在のクラスタープロパティー設定から作成された **pcs property set** コマンドが表示されます。このコマンドを使用すると、設定済みのクラスタープロパティーを別のシステム上に再作成できます。
  - **--output-format=json** を指定すると、設定済みのクラスタープロパティーが JSON 形式で表示されます。
  - 設定済みのクラスタープロパティーをプレーンテキスト形式で表示するには、**output-format=text** を指定します。これは、このオプションのデフォルト値です。
- **pcs propertydefaults** コマンド。これは、非推奨となった **pcs property --defaults** オプションに代わるものです。
- **pcs property describe** コマンド。これは、クラスタープロパティーの意味を説明します。

Bugzilla:2166289

4.8. 動的プログラミング言語、WEB サーバー、およびデータベースサーバー

新しい nodejs:20 モジュールストリームが完全にサポートされるようになりました。

以前はテクノロジープレビューとして利用できた新しい **nodejs:20** モジュールストリームが、RHEA-2023:7249 アドバイザリーのリリースに伴い、フルサポート対象になりました。**nodejs:20** モジュールストリームでは、LTS (Long Term Support) バージョンの **Node.js 20.9** が提供されるようになりました。

RHEL 8.9 に含まれる **Node.js 20** は、RHEL 8.7 以降で利用可能な **Node.js 18** に比べて、多数の新機能、バグ修正、セキュリティー修正、およびパフォーマンスの改善を提供します。

主な変更点は、以下のとおりです。

- **V8** JavaScript エンジンがバージョン 11.3 にアップグレードされました。
- **npm** パッケージマネージャーがバージョン 9.8.0 にアップグレードされました。
- **Node.js** に、新しい実験的な権限モデルが導入されています。
- **Node.js** に、新しい実験的な Single Executable Application (SEA) 機能が導入されています。
- **Node.js** は、Experimental ECMAScript モジュール (ESM) ローダーの改良を提供します。
- **Node.js 18** で実験的な **node:test** モジュールとして導入されたネイティブテストランナーは、現在は安定していると考えられています。

nodejs:20 モジュールストリームをインストールするには、以下を使用します。

```
# yum module install nodejs:20
```

nodejs:18 ストリームからアップグレードする場合は、後のストリームへの切り替え を参照してください。

nodejs Application Streams のサポート期間の詳細は、Red Hat Enterprise Linux Application Streams のライフサイクル を参照してください。

Bugzilla:2186718

Python tarfile 抽出関数への新しい filter 引数

CVE-2007-4559 の問題を軽減するために、Python は **tarfile** 抽出関数に **filter** 引数を追加します。この引数により、安全性を高めるために **tar** 機能をオフにすることができます (CVE-2007-4559 ディレクトリートラバーサル攻撃のブロックを含む)。フィルターが指定されていない場合、RHEL ではデフォルトで、最も安全ですが制限が最も高い **'data'** フィルターが使用されます。さらに、アプリケーションが影響を受けると、Python は警告を発行します。

警告を非表示にする手順などの詳細は、ナレッジベースの記事 Mitigation of directory traversal attack in the Python tarfile library (CVE-2007-4559) を参照してください。

Jira:RHELDOCS-16405[1]

HTTP::Tiny Perl モジュールは、デフォルトで TLS 証明書を検証するようになる

HTTPS の使用時に TLS 証明書を検証するために、**HTTP::Tiny** Perl モジュールの **verify_SSL** オプションのデフォルト値が **0** から **1** に変更されました。この変更により、**HTTP::Tiny** の CVE-2023-31486 と CPAN Perl モジュールの CVE-2023-31484 が修正されます。

TLS 検証のサポートを利用できるようにするために、この更新では次の依存関係を **perl-HTTP-Tiny** パッケージに追加します。

- **perl-IO-Socket-SSL**
- **perl-Mozilla-CA**
- **perl-Net-SSLeay**

Bugzilla:2228409[1]

メールアドレスの解析を制御するための Python の新しい環境変数

CVE-2023-27043 の問題を軽減するために、メールアドレスをより厳密に解析するための後方互換性のない変更が Python 3 に導入されました。

RHSA-2024:0256 の更新では、新しい **PYTHON_EMAIL_DISABLE_STRICT_ADDR_PARSING** 環境変数が導入されています。この変数を **true** に設定すると、比較的厳密ではない以前の解析動作が、システム全体のデフォルトになります。

```
export PYTHON_EMAIL_DISABLE_STRICT_ADDR_PARSING=true
```

ただし、該当する関数を個別に呼び出すと、より厳密な動作が有効になる可能性があります。

次の内容で **/etc/python/email.cfg** 設定ファイルを作成しても、同じ結果を得ることができます。

```
[email_addr_parsing]
PYTHON_EMAIL_DISABLE_STRICT_ADDR_PARSING = true
```

詳細は、ナレッジベース記事 Mitigation of CVE-2023-27043 introducing stricter parsing of email addresses in Python を参照してください。

Jira:RHELDOCS-17369[1]

4.9. コンパイラーおよび開発ツール

glibc の Intel® Xeon® v5 ベースのハードウェアでの文字列およびメモリールーチンのパフォーマンスが向上

以前は、文字列およびメモリールーチン用に **glibc** によって使用されるデフォルトのキャッシュ量により、Intel® Xeon® v5 ベースのシステムで、パフォーマンスが予想よりも低下していました。今回の更新では、パフォーマンスを向上させるために使用するキャッシュの量が調整されました。

Bugzilla:2180462

GCC はレジスター引数の保持をサポートするようになる

今回の更新により、引数レジスターの内容をスタックに保存し、適切な Call Frame Information (CFI) を生成して、アンワインダーがパフォーマンスに悪影響を与えることなく CFI を特定できるようになりました。

Bugzilla:2168205[1]

新しい GCC Toolset 13

GCC Toolset 13 は、最新バージョンの開発ツールを提供するコンパイラーツールセットです。これは、AppStream リポジトリー内の Software Collection の形式で Application Stream として利用できます。

GCC コンパイラーがバージョン 13.1.1 に更新され、アップストリームの GCC で利用できる多くのバグ修正と機能拡張が提供されています。

次のツールとバージョンが GCC Toolset 13 によって提供されます。

ツール	バージョン
GCC	13.1.1
GDB	12.1
binutils	2.40
dwz	0.14
annobin	12.20

GCC Toolset 13 をインストールするには、root として次のコマンドを実行します。

```
# yum install gcc-toolset-13
```

GCC Toolset 13 からツールを実行するには、以下を使用します。

```
$ scl enable gcc-toolset-13 tool
```

GCC Toolset 13 のツールバージョンがこれらのツールのシステムバージョンをオーバーライドするシェルセッションを実行するには、以下を使用します。

```
$ scl enable gcc-toolset-13 bash
```

詳細は、https://access.redhat.com/documentation/ja-jp/red_hat_enterprise_linux/8/html/developing_c_and_cpp_applications_in_rhel_8/additional-toolsets-for-development_developing-applications#gcc-toolset-13_assembly_additional-toolsets-for-development[GCC Toolset 13] および GCC Toolset の使用 を参照してください。

Bugzilla:2171898[1]、Bugzilla:2171928、Bugzilla:2188490

GCC Toolset 13: GCC がバージョン 13.1.1 にリベース

GCC Toolset 13 では、GNU Compiler Collection (GCC) がバージョン 13.1.1 に更新されました。主な変更点は、以下のとおりです。

一般的な改善

- OpenMP:
  - OpenMP 5.0: Fortran は、いくつかの非長方形ループネストをサポートするようになりました。このようなサポートは、GCC 11 で C/C++ に追加されました。

  - 多くの OpenMP 5.1 機能が追加されました。
  - OpenMP 5.2 機能の初期サポートが追加されました。
- 新しいデバッグ情報圧縮オプション値 **-gz=zstd** が利用できるようになりました。
- **-Ofast**、**-ffast-math**、および **-funsafe-math-optimizations** オプションでは、**-shared** オプションを使用して共有オブジェクトを生成するときに、浮動小数点環境を変更するためのスタートアップコードが追加されなくなりました。
- GCC は、静的分析ツール (GCC の **-fanalyzer** など) の結果をキャプチャーするのに適した JSON ベース形式の、Static Analysis Results Interchange Format (SARIF) を使用して、診断を出力できるようになりました。SARIF を使用して、他の GCC 警告やエラーを機械可読形式でキャプチャーすることもできます。
- リンクタイム最適化の改善が実装されました。

新しい言語と言語固有の改善

C ファミリー:

- 新しい **-Wxor-used-as-pow** オプションは、ユーザーが指数を意図した可能性がある排他的論理和 (**^**) 演算子の使用について警告します。
- ファイル記述子である **int** 引数を文書化するために、3 つの新しい関数属性が追加されました。
  - **attribute((fd_arg(N)))**
  - **attribute((fd_arg_read(N)))**
  - **attribute((fd_arg_write(N)))**

  これらの属性は、ファイル記述子の誤用を検出するために **-fanalyzer** によっても使用されます。
- 新しいステートメント属性、**attribute((assume(EXPR)));** が、C++23 移植性の前提のために追加されました。この属性は、C または以前の C++ でもサポートされています。
- GCC は、配列の要素にアクセスする目的で、構造体の最後の配列を柔軟な配列メンバーとして扱うタイミングを制御できるようになりました。デフォルトでは、集合体の最後の配列はすべて柔軟な配列メンバーとして扱われます。新しいコマンドラインオプション **-fstrict-flex-arrays** を使用して、どの配列メンバーを柔軟な配列として扱うかを制御します。

C:

- いくつかの C23 機能が実装されました。
  - **nullptr** 定数が導入されました。
  - 基礎となる型を指定するために列挙が強化されました。
  - 可変個引数パラメーターリストの要件が緩和されました。
  - オブジェクト定義の型推論を有効にする **auto** 機能が導入されました。
  - オブジェクト定義に **constexpr** 指定子が導入されました。
  - 複合リテラル用のストレージクラス指定子が導入されました。

  - **typeof** オブジェクト (以前はエクステンションとしてサポート) と **typeof_unqual** オブジェクトが導入されました。
  - 新しいキーワード **alignas**、**alignof**、**bool**、**false**、**static_assert**、**thread_local**、および **true** を追加しました。
  - 関数が呼び出し元に実行を返さないことを指定する **[[noreturn]]** 属性を追加しました。
  - 空のイニシャライザー括弧のサポートが追加されました。
  - **STDC_VERSION_*_H** ヘッダーバージョンマクロのサポートが追加されました。
  - **ATOMIC_VAR_INIT** マクロを削除しました。
  - **<stddef.h>** ヘッダーに **unreachable** マクロを追加しました。
  - トライグラフを削除しました。
  - プロトタイプ化されていない関数を削除しました。
  - **%wN** および **%wfN** 形式の長さ修飾子の **-Wformat** オプションを使用した **printf** および **scanf** 形式のチェックを追加しました。
  - Unicode Standard Annex (UAX) 31 の識別子構文のサポートが追加されました。
  - C23 で採用されている既存の機能は、C23 要件に従うように調整されており、**-std=c2x -Wpedantic** オプションを使用して診断されることはありません。
- 新しい **-Wenum-int-mismatch** オプションは、列挙型と整数型の間の不一致について警告します。

C++:

- **-fexcess-precision** オプションを使用して、excess precision サポートを実装しました。これは、**-std=c++17** のような厳密な標準モードではデフォルトで有効化されています。デフォルトは **-fexcess-precision=standard** になります。**-std=gnu++20** のような GNU 標準モードでは、デフォルトは **-fexcess-precision=fast** となり、以前の動作が復元されます。**-fexcess-precision** オプションは、次のアーキテクチャーに影響します。
  - x87 演算を使用する Intel 32 および 64 ビット、場合によっては Motorola 68000 では、**float** と **double** 式が **long double** 精度で評価されます。
  - 64 ビット IBM Z システムでは、**float** 式が **double** 精度で評価されます。
  - **std::float16_t** または **std::bfloat16_t** 型をサポートするいくつかのアーキテクチャーでは、これらの型は **float** 精度で評価されます。
- 以下を含む C++23 の実験的サポートが改善されました。
  - 複合ステートメントの末尾にラベルのサポートが追加されました。
  - 一時オブジェクトへの参照バインディングを検出するための型特性を追加しました。
  - 揮発性複合操作のサポートが再導入されました。
  - **#warning** ディレクティブのサポートが追加されました。
  - 区切られたエスケープシーケンスのサポートが追加されました。

  - 名前付きユニバーサル文字エスケープのサポートが追加されました。
  - **char8_t** タイプの互換性と移植性に関する修正を追加しました。
  - 静的 **operator()** 関数オブジェクトを追加しました。
  - 暗黙的なムーブを簡略化しました。
  - 式内の等価性の書き換えは、以前より互換性を破壊しにくくなりました。
  - エンコード不可能なワイド文字リテラルとワイド複数文字リテラルを削除しました。
  - **constexpr** 関数の制限をいくつか緩和しました。
  - 拡張浮動小数点型と標準名。
  - 移植可能な前提条件を実装しました。
  - 移植可能なソースファイルのエンコード標準として UTF-8 のサポートを追加しました。
  - 静的 **operator[]** の添字演算子の多次元サポートを追加しました。
- 新しい警告:
  - **-Wself-move** は、**std::move** を使用して値がそれ自体に移動されると警告します。
  - **-Wdangling-reference** は、有効期間が終了した一時オブジェクトに参照がバインドされている場合に警告します。
  - **-Wpessimizing-move** および **-Wredundant-move** 警告は、より多くのコンテキストで警告するように拡張されました。
- 新しい **-nostdlib++** オプションを使用すると、C++ 標準ライブラリーで暗黙的にリンクせずに、**g++** とのリンクが可能になります。

libstdc++ ランタイムライブラリーの変更

- 以下を含む C++20 の実験的サポートが改善されました。
  - **<format>** ヘッダーと **std::format** 関数を追加しました。
  - **<chrono>** ヘッダーに、**std::chrono::utc_clock** クロック、その他のクロック、タイムゾーン、および **std::format** 関数のサポートが追加されました。
- 以下を含む C++23 の実験的サポートが改善されました。
  - **<ranges>** ヘッダーへの追加:
    views::zip、**views::zip_transform**、**views::adjacent**、**views::adjacent_transform**、**views::pairwise**、**views::slide**、**views::chunk**、**views::chunk_by**、**views::repeat**、**views::chunk_by**、**views::cartesian_product**、**views::as_rvalue**、**views::enumerate**, **views::as_const**
  - **<algorithm>** ヘッダーへの追加:
    ranges::contains、**ranges::contains_subrange**、**ranges::iota**、**ranges::find_last**、**ranges::find_last_if**、**ranges::find_last_if_not**、**ranges::fold_left**、**ranges::fold_left_first**、**ranges::fold_right**、**ranges::fold_right_last**、**ranges::fold_left_with_iter**、**ranges::fold_left_first_with_iter**

  - **std::expected** クラステンプレートのモナド操作のサポート。
  - **constexpr** 修飾子を **std::bitset**、**std::to_chars**、および **std::from_chars** 関数に追加しました。
  - 拡張浮動小数点型のライブラリーサポートを追加しました。
- Library Fundamentals Technical Specification (TS) のバージョン 3 から **<experimental/scope>** ヘッダーのサポートが追加されました。
- Concurrency TS のバージョン 2 から **<experimental/synchronized_value>** ヘッダーのサポートが追加されました。
- フリースタンディング環境で以前は利用できなかった多くの機能のサポートが追加されました。以下に例を示します。
  - **std::tuple** クラステンプレートをフリースタンディング環境でのコンパイルに使用できるようになりました。
  - **libstdc++** ライブラリーは、**std::array** や **std::string_view** などのコンポーネントをフリースタンディング環境のサブセットに追加します。
  - **libstdc++** ライブラリーは **-ffreestanding** コンパイラーオプションを尊重するようになったため、**libstdc++** ライブラリーのフリースタンディング環境でのインストールを別途ビルドする必要がなくなりました。**-ffreestanding** を指定してコンパイルすると、**libstdc++** ライブラリーが完全なホスト型実装としてビルドされた場合でも、フリースタンディング環境のサブセットで利用可能な機能が制限されます。

新しいターゲットとターゲット固有の改善

64 ビット ARM アーキテクチャー

- **-march=** オプションの **armv9.1-a**、**armv9.2-a**、および **armv9.3-a** 引数のサポートが追加されました。

32 ビットおよび 64 ビットの AMD および Intel アーキテクチャー:

- C と C++ の両方の場合、**__bf16** 型は、Streaming SIMD Extensions 2 以降が有効になっているシステムでサポートされます。
- 実際の **__bf16** 型が **AVX512BF16** 命令組み込みに使用されるようになりました。以前は、short の typedef である **__bfloat16** が使用されていました。GCC 12 を GCC 13 にアップグレードするときに、**AVX512BF16** 関連のソースコードを調整してください。
- 次の Intel 命令をサポートするための新しいInstruction Set Architecture (ISA) エクステンションが追加されました。
  - **AVX-IFMA** の命令組み込みは、**-mavxifma** コンパイラースイッチを通じて使用できます。
  - **AVX-VNNI-INT8** の命令組み込みは、**-mavxvnniint8** コンパイラースイッチを通じて使用できます。
  - **AVX-NE-CONVERT** の命令組み込みは、**-mavxneconvert** コンパイラースイッチを通じて使用できます。
  - **CMPccXADD** の命令組み込みは、**-mcmpccxadd** コンパイラースイッチを通じて使用できます。

  - **AMX-FP16** の命令組み込みは、**-mamx-fp16** コンパイラースイッチを通じて使用できます。
  - **PREFETCHI** の命令組み込みは、**-mprefetchi** コンパイラースイッチを通じて使用できます。
  - **RAO-INT** の命令組み込みは、**-mraoint** コンパイラースイッチを通じて使用できます。
  - **AMX-COMPLEX** の命令組み込みは、**-mamx-complex** コンパイラースイッチを通じて使用できます。
- GCC は、**-march=znver4** コンパイラースイッチを通じて、**znver4** コアに基づく AMD CPU をサポートするようになりました。このスイッチにより、GCC は自動ベクトル化時に 512 ビットベクトルの使用を考慮します。

静的アナライザーの改善

- 静的アナライザーは 20 件の新しい警告を取得しました。
  - **-Wanalyzer-allocation-size**
  - **-Wanalyzer-deref-before-check**
  - **-Wanalyzer-exposure-through-uninit-copy**
  - **-Wanalyzer-imprecise-fp-arithmetic**
  - **-Wanalyzer-infinite-recursion**
  - **-Wanalyzer-jump-through-null**
  - **-Wanalyzer-out-of-bounds**
  - **-Wanalyzer-putenv-of-auto-var**
  - **-Wanalyzer-tainted-assertion**
  - ファイル記述子の誤用に関する 7 つの新しい警告:
    - **-Wanalyzer-fd-access-mode-mismatch**
    - **-Wanalyzer-fd-double-close**
    - **-Wanalyzer-fd-leak**
    - **-Wanalyzer-fd-phase-mismatch** (例: ソケットで **listen** を呼び出す前のソケットでの **accept** の呼び出し)
    - **-Wanalyzer-fd-type-mismatch** (例: データグラムソケットでのストリームソケット操作の使用)
    - **-Wanalyzer-fd-use-after-close**
    - **-Wanalyzer-fd-use-without-check**
      - また、**open**、**close**、**creat**、**dup**、**dup2**、**dup3**、**pipe**、**pipe2**、**read**、および **write** 関数の動作の特殊ケーシングの処理も実装されました。

- **<stdarg.h>** ヘッダーの誤用に関する 4 つの新しい警告:
  - **-Wanalyzer-va-list-leak** は、**va_start** マクロまたは **va_copy** マクロの後に **va_end** マクロがないことを警告します。
  - **-Wanalyzer-va-list-use-after-va-end** は、**va_end** マクロが呼び出された **va_list** オブジェクトタイプで使用されている **va_arg** または **va_copy** マクロについて警告します。
  - **-Wanalyzer-va-arg-type-mismatch** タイプは、プロシージャー間の実行パスでの **va_arg** マクロの使用状況を、実際に可変個引数呼び出しに渡されたパラメーターの型と照合してチェックします。
  - **-Wanalyzer-va-list-exhausted** は、プロシージャー間実行パス内の **va_list** オブジェクトタイプで **va_arg** マクロが何度も使用されている場合に警告します。

- その他多数の改善。

後方互換性のない変更

C++ の場合、**std::cout**、**std::cin** などのグローバル iostream オブジェクトの構築は、**<iostream>** ヘッダーを含むすべてのソースファイルではなく、標準ライブラリー内で行われるようになりました。この変更により、C++ プログラムの起動パフォーマンスが向上しますが、ランタイムに正しいバージョンの **libstdc++.so** が使用されない場合、GCC 13.1 でコンパイルされたコードがクラッシュすることになります。ランタイムに正しい **libstdc++.so** を使用する方法の詳細は、ドキュメント を参照してください。将来の GCC リリースではこの問題が軽減され、互換性のない以前の **libstdc++.so** ではプログラムをまったく実行できなくなります。

Bugzilla:2172091[1]

GCC Toolset 13: annobin がバージョン 12.20 にリベース

GCC Toolset 13 は、**annobin** パッケージのバージョン 12.20 を提供します。主な機能拡張は、次のとおりです。

- **annobin** ノートを別のデバッグ情報ファイルに移動するためのサポートが追加されました。これにより、実行可能バイナリーのサイズが縮小されます。
- 新しい小さな note フォーマットのサポートが追加されたことで、個別の debuginfo ファイルのサイズが縮小され、これらのファイルの作成にかかった時間が短縮されました。

Bugzilla:2171923[1]

GCC Toolset 13: GDB がバージョン 12.1 にリベース

GCC Toolset 13 は、GDB バージョン 12.1 を提供します。

主なバグ修正と機能拡張は、以下のとおりです。

- GDB では、デフォルトでソースコードと逆アセンブラーのスタイルが設定されるようになりました。スタイリングが GDB の自動化またはスクリプト作成を妨げる場合は、**maint set gnu-source-highlight enabled off** および **maint set style disassembler enabled off** コマンドを使用してスタイル設定を無効にできます。
- GDB は、内部エラーが発生するたびにバックトレースを表示するようになりました。これがスクリプトまたは自動化に影響する場合は、**maint set backtrace-on-fatal-signal off** コマンドを使用して、この機能を無効にすることができます。

C/C++ の改善:

- GDB は、C++ テンプレートに関係する関数または型を関数のオーバーロードと同様に扱うようになりました。パラメーターリストを省略して、複数のテンプレートタイプで構成される型や関数などのテンプレート関数のファミリーにブレークポイントを設定できます。**タブ** 補完にも同様の改善が加えられました。

ターミナルユーザーインターフェイス (TUI):

- **tui layout**
  tui focus

  tui refresh

  tui window height
  これらは、それぞれ古い **layout**、**focus**、**refresh**、**winheight** TUI コマンドの新しい名前です。古い名前は、これらの新しいコマンドのエイリアスとしてまだ存在しています。

- **tui window width**
  winwidth

  ウィンドウが水平モードでレイアウトされている場合、新しい **tui window width** コマンドまたは **winwidth** エイリアスを使用して、TUI ウィンドウの幅を調整します。

- **info win**
  このコマンドの出力には、TUI ウィンドウの幅に関する情報が含まれるようになりました。

Machine Interface (MI) の変更:

- MI インタープリターのデフォルトバージョンが 4 (-i=mi4) になりました。

- フラグのない **-add-inferior** コマンドは、現在の下位コマンドの接続を継承するようになりました。これにより、バージョン 10 より前の GDB の動作が復元されます。

- **-add-inferior** コマンドは、接続なしで新しい下位コマンドを起動させる **--no-connection** フラグを受け入れるようになりました。

- ブレークポイント出力の **script** フィールド (MI 3 以前では構文的に不正確) は、MI 4 ではリストになりました。これは次のコマンドとイベントに影響します。

  - **-break-insert**

  - **-break-info**

  - **=breakpoint-created**

  - **=breakpoint-modified**
    以前の MI バージョンでの新しい動作を有効にするには、**-fix-breakpoint-script-output** コマンドを使用します。

新しいコマンド:

- **maint set internal-error backtrace [on|off]**
  maint show internal-error backtrace

  maint set internal-warning backtrace [on|off]

maint show internal-warning backtrace

GDB は、内部エラーまたは内部警告が発生したときに、自身のバックトレースを出力できるようになりました。これは、内部エラーの場合はデフォルトで有効化され、内部警告の場合はデフォルトで無効化されています。

- **exit**
  既存の **quit** コマンドに加えて、新しい **exit** コマンドを使用して GDB を終了できます。

- **maint set gnu-source-highlight enabled [on|off]**
  maint show gnu-source-highlight enabled
  ソースコードにスタイリングを追加するために、GNU Source Highlight ライブラリーを有効または無効化します。無効にすると、ライブラリーは利用可能であっても使用されません。GNU Source Highlight ライブラリーが使用されない場合は、代わりに Python Pygments ライブラリーが使用されます。

- **set suppress-cli-notifications [on|off]**
  show suppress-cli-notifications

  CLI に対して通知の出力を抑制するかどうかを制御します。CLI 通知は、選択したコンテキスト (現在の下位、スレッド、フレームなど) を変更したとき、またはデバッグ中のプログラムが停止したときに (ブレークポイントに到達した、ソースステッピングの完了、または割り込みなどにより) 発生します。

- **set style disassembler enabled [on|off]**
  show style disassembler enabled

  有効化すると、GDB が Python サポートでコンパイルされており、Python Pygments パッケージが利用可能な場合、コマンドは逆アセンブラー出力にスタイリングを適用します。

変更したコマンド:

- **set logging [on|off]**
  非推奨となり、**set logging enabled [on|off]** コマンドに置き換えられました。

- **print**
  /x のような基数変更形式を使用した浮動小数点値の出力は、目的の基数で値の基礎となるバイトを表示するように変更されました。

- **clone-inferior**
  clone-inferior コマンドにより、**TTY**、**CMD**、および **ARGs** の設定が、元の下位設定から新しい設定にコピーされるようになりました。**set environment** コマンドまたは **unset environment** コマンドを使用して加えられた環境変数へのすべての変更も、新しい下位環境変数にコピーされます。

Python API:

- 新しい **gdb.add_history()** 関数は、**gdb.Value** オブジェクトを取り、それが表す値を GDB の履歴リストに追加します。この関数は、履歴リスト内の新しい項目のインデックスである整数を返します。

- 新しい **gdb.history_count()** 関数は、GDB の値履歴内の値の数を返します。

- 新しい **gdb.events.gdb_exiting** イベントは、GDB 終了コードの値を含む読み取り専用属性 **exit_code** を持つ **gdb.GdbExitingEvent** オブジェクトを使用して呼び出されます。このイベントは、GDB が終了する前の、GDB が内部状態のクリーンアップを開始する前にトリガーされます。

- 新しい **gdb.architecture_names()** 関数は、考えられるすべての **Architecture.name()** 値を含むリストを返します。各エントリーは文字列です。
- 新しい **gdb.Architecture.integer_type()** 関数は、サイズと符号付きかどうかを指定して整数型を返します。
- 新しい **gdb.TargetConnection** オブジェクトタイプは、(**info connection** コマンドで表示される) 接続を表します。サブクラス **gdb.RemoteTargetConnection** は、**remote** 接続および **extended-remote** 接続を表します。
- **gdb.Inferior** 型には、**gdb.TargetConnection** オブジェクトのインスタンスである **connection** プロパティーがあり、この下位型によって使用される接続になります。下層に接続がない場合、これは **None** にすることができます。
- 新しい **gdb.events.connection_removed** イベントレジストリーは、接続が GDB から削除されると **gdb.ConnectionEvent** イベントを発行します。このイベントには、**connection** プロパティー、つまり削除される接続の **gdb.TargetConnection** オブジェクトがあります。
- 新しい **gdb.connections()** 関数は、現在アクティブなすべての接続のリストを返します。
- 新しい **gdb.RemoteTargetConnection.send_packet(PACKET)** メソッドは、既存の **maint packet** CLI コマンドと同等です。これを使用して、指定したパケットをリモートターゲットに送信できます。
- 新しい **gdb.host_charset()** 関数は、現在のホスト文字セットの名前を文字列として返します。
- 新しい**gdb.set_parameter(NAME, VALUE)** 関数は、GDB パラメーター **NAME** を **VALUE** に設定します。
- 新しい **gdb.with_parameter (NAME、VALUE)** 関数は、GDB パラメーター **NAME** を一時的に **VALUE** に設定してから、コンテキストが終了するとリセットするコンテキストマネージャーを返します。
- **gdb.Value.format_string** メソッドは、ブール値である **styling** 引数を取るようになりました。**true** の場合、返される文字列には、スタイリングを適用するためのエスケープシーケンスを含めることができます。スタイリングは、GDB でスタイリングがオンになっている場合にのみ存在します (**help set styling** を参照してください)。**false** の場合 (**スタイル** 引数が指定されていない場合のデフォルト)、返される文字列にはスタイリングは適用されません。
- 新しい読み取り専用属性 **gdb.InferiorThread.details** は、追加のターゲット固有のスレッド状態情報を含む文字列か、そのような追加情報がない場合は **None** になります。
- 新しい読み取り専用属性 **gdb.Type.is_scalar** は、スカラー型の場合は **True**、その他すべての型の場合は **False** です。
- 新しい読み取り専用属性 **gdb.Type.is_signed** は、**Type.is_scalar** が **True** の場合にのみ読み取られる必要があり、符号付き型の場合は **True**、その他すべての型の場合は **False** になります。非スカラー型に対してこの属性を読み取ろうとすると、**ValueError** が発生します。
- Python で実装された GDB および MI コマンドを追加できるようになりました。

詳細は、アップストリームのリリースノートを参照してください。

What has changed in GDB?

Bugzilla:2172095[1]

GCC Toolset 13: binutils がバージョン 2.40 にリベース

GCC Toolset 13 は、**binutils** パッケージバージョン 2.40 を提供します。主な機能拡張は、次のとおりです。

リンカー:

- リンカーの新しい **-w** (**--no-warnings**) コマンドラインオプションは、警告メッセージやエラーメッセージの生成を抑制します。これは、動作しないことがわかっているバイナリーを作成する必要がある場合に役立ちます。
- ELF リンカーは、次の場合に警告メッセージを生成するようになりました。
  - スタックが実行可能な場合。
  - **Read**、**Write**、**eXecute** の 3 つのパーミッションセットをすべて備えたメモリー常駐セグメントを作成する場合。
  - **eXecute** パーミッションセットを使用してスレッドローカルデータセグメントを作成する場合。
    --no-warn-exec-stack または **--no-warn-rwx-segments** オプションを使用すると、これらの警告を無効にできます。
- リンカーは、作成するバイナリーに任意の JSON 形式のメタデータを挿入できるようになりました。

その他のツール:

- Portable Executable (PE) 形式ファイルのファイルヘッダーとセクションヘッダーのフィールドを表示する、**objdump** ツールの新しい **--private** オプション。
- ELF ファイルから ELF セクションヘッダーを削除するための、**objcopy** ユーティリティーおよび **strip** ユーティリティー用の新しい **--strip-section-headers** コマンドラインオプション。
- **objdump** ユーティリティーの新しい **--show-all-symbols** コマンドラインオプションは、アドレスに一致する最初のシンボルのみを表示するデフォルト機能とは対照的に、逆アセンブル時に指定されたアドレスに一致するすべてのシンボルを表示します。
- **nm** ユーティリティーに新しい **-W** (**--no-weak**) オプションを追加し、弱いシンボルを無視します。
- **objdump** ユーティリティーは、一部のアーキテクチャーの逆アセンブラー出力の構文強調表示をサポートするようになりました。**--disassembler-color=MODE** コマンドラインオプションを使用します。**MODE** は、次のいずれかになります。
  - **off**
  - **color** - このオプションは、すべてのターミナルエミュレーターでサポートされています。
  - **extended-color** - このオプションは、すべてのターミナルエミュレーターでサポートされていない 8 ビットカラーを使用します。

Bugzilla:2171924[1]

GCC Toolset 13: annobin がバージョン 12.20 にリベース

GCC Toolset 13 は、**annobin** パッケージのバージョン 12.20 を提供します。主な機能拡張は、次のとおりです。

- **annobin** ノートを別のデバッグ情報ファイルに移動するためのサポートが追加されました。これにより、実行可能バイナリーのサイズが縮小されます。
- 新しい小さなメモ形式のサポートが追加されたことで、個別の debuginfo ファイルのサイズが縮小され、これらのファイルの作成にかかった時間が短縮されました。

Bugzilla:2171921[1]

Valgrind がバージョン 3.21.0 にリベース

Valgrind がバージョン 3.21.0 に更新されました。主な機能拡張は、次のとおりです。

- **--vgdb-stop-at=event1,event2,...** オプションの新しい **abexit** 値は、ゼロ以外の終了コードなどでプログラムが異常終了したときに **gdbserver** ユーティリティーに通知します。
- 新しい **--enable-debuginfod=[yes|no]** オプションは、**DEBUGINFOD_URLS** 環境変数にリストされている **debuginfod** サーバーを使用して、Valgrind で実行されているプログラムに不足している DWARF debuginfo 情報を取得するように Valgrind に指示します。このオプションのデフォルト値は **yes** です。

注記

DEBUGINFOD_URLS 環境変数は、デフォルトでは設定されません。

- **vgdb** ユーティリティーは、**--multi** オプションを指定して呼び出された場合に、拡張リモートプロトコルをサポートするようになりました。このモードでは GDB **run** コマンドがサポートされているため、1 つのターミナルから GDB と Valgrind を実行できます。
- **--realloc-zero-bytes-frees=[yes|no]** オプションを使用すると、**malloc()** 呼び出しをインターセプトするツールのサイズ 0 の **realloc()** 関数の動作を変更できます。
- **memcheck** ツールは、サイズ 0 の **realloc()** 関数の使用のチェックを実行するようになりました。この機能を無効にするには、新しい **--show-realloc-size-zero=[yes|no]** スイッチを使用します。
- **helgrind** ツールの新しい **--history-backtrace-size=value** オプションを使用して、以前のアクセスのスタックトレースに記録するエントリーの数を設定できます。
- **--cache-sim=[yes|no] cachegrind** オプションはデフォルトで **no** になり、その結果、デフォルトでは命令キャッシュ読み取りイベントのみが収集されるようになりました。
- **cg_annotate**、**cg_diff**、および **cg_merge cachegrind** ユーティリティーのソースコードが書き直されたため、ユーティリティーのコマンドラインオプションの処理がより柔軟になりました。たとえば、**--show-percs** と **--no-show-percs** オプションのほか、既存の **--show-percs=yes** と **--show-percs=no** オプションもサポートされるようになりました。
- **cg_annotate cachegrind** ユーティリティーは、差分 (**--diff**、**--mod-filename**、および **--mod-funcname** オプションを使用) とマージ (複数のデータファイルを渡すことによる) をサポートするようになりました。さらに、**cg_annotate** は、ファイルおよび関数レベルでより多くの情報を提供するようになりました。
- **DHAT** ツールに対する新しいユーザー要求により、メモリーブロックのアクセスカウントヒストグラムの 1024 バイト制限をオーバーライドできるようになります。

次の新しいアーキテクチャー固有の命令セットがサポートされるようになりました。

- 64 ット ARM:
  - v8.2 スカラーおよびベクトルの Floating-point Absolute Difference (FABD)、Floating-point Absolute Compare Greater than or Equal (FACGE)、Floating-point Absolute Compare Greater Than (FACGT)、および Floating-point Add (FADD) 命令。
  - v8.2 Floating-point (FP) 比較命令と条件付き比較命令。
  - v8.2 Floating-point (FP) 比較命令のゼロバリアント。
- 64-ビット IBM Z:
  - **miscellaneous-instruction-extensions facility 3** および **vector-enhancements facility 2** のサポート。これにより、**-march=arch13** または **-march=z15** オプションを使用してコンパイルされたプログラムを Valgrind で実行できるようになります。
- IBM Power:
  - ISA 3.1 のサポートが完了しました。
  - ISA 3.0 は、deliver a random number (darn) 命令をサポートするようになりました。
  - ISA 3.0 は、System Call Vectored (scv) 命令をサポートするようになりました。
  - ISA 3.0 は、コピー、貼り付け、および cpabort 命令をサポートするようになりました。

Bugzilla:2124345

systemtap がバージョン 4.9 にリベース

systemtap パッケージがバージョン 4.9 にアップグレードされました。主な変更点は、以下のとおりです。

- 新しい Language-Server-Protocol (LSP) バックエンドにより、LSP 対応エディターでの **systemtap** スクリプトのインタラクティブなドラフト作成が容易になります。
- Python/Jupyter インタラクティブノートブックフロントエンドへのアクセス。
- DWARF 5 ビットフィールドの処理が改善されました。

Bugzilla:2186932

elfutils がバージョン 0.189 にリベース

elfutils パッケージがバージョン 0.189 に更新されました。主な改善点とバグ修正は次のとおりです。

libelf

elf_compress ツールは、**ELFCOMPRESS_ZSTD** ELF 圧縮タイプをサポートするようになりました。

libdwfl

dwfl_module_return_value_location 関数は、**DW_TAG_unspecified_type** タイプのタグを指す DWARF Information Entries (DIEs) に対して 0 (戻り値のタイプなし) を返すようになりました。

eu-elfcompress

-t および **--type=** オプションは、**zstd** 引数を介して Zstandard (**zstd**) 圧縮形式をサポートするようになりました。

Bugzilla:2182060

libpfm がバージョン 4.13 にリベース

libpfm パッケージがバージョン 4.13 に更新されました。この更新により、**libpfm** は、次のプロセッサーマイクロアーキテクチャーのパフォーマンス監視ハードウェアネイティブイベントにアクセスできるようになります。

- AMD Zen 4
- ARM Neoverse N1
- ARM Neoverse N2
- ARM Neoverse V1
- ARM Neoverse V2
- 第 4 世代 Intel® Xeon® スケーラブルプロセッサー
- IBM z16

Bugzilla:2185653, Bugzilla:2111987, Bugzilla:2111966, Bugzilla:2111973, Bugzilla:2109907, Bugzilla:2111981, Bugzilla:2047725

papi は、新しいプロセッサーマイクロアーキテクチャーをサポートする

この機能拡張により、次のプロセッサーマイクロアーキテクチャー上の **papi** イベントプリセットを使用して、パフォーマンス監視ハードウェアにアクセスできるようになります。

- ARM Neoverse N1
- ARM Neoverse N2
- ARM Neoverse V1
- ARM Neoverse V2

Bugzilla:2111982[1]、Bugzilla:2111988

papi は、64 ビット ARM の高速パフォーマンスイベントカウント読み取り操作をサポートするようになる

以前の 64 ビット ARM プロセッサーでは、すべてのパフォーマンスイベントカウンターの読み取り操作で、リソースを大量に消費するシステムコールを使用する必要がありました。**papi** は、64 ビット ARM 用に更新され、パフォーマンスカウンターで自身を監視するプロセスが、パフォーマンスイベントカウンターのより高速なユーザー空間読み取りを使用できるようになりました。**/proc/sys/kernel/perf_user_access** パラメーターを 1 に設定すると、**papi** が 2 つのカウンターを読み取るための平均クロックサイクル数が 724 サイクルから 29 サイクルに減少します。

Bugzilla:2161146[1]

LLVM Toolset がバージョン 16.0.6 にリベース

LLVM Toolset がバージョン 16.0.6 に更新されました。

主な機能拡張は、次のとおりです。

- 最適化の改善

- 新しい CPU 拡張のサポート
- 新しい C++ バージョンへのサポートの改善

後方互換性のない注目すべき変更は次のとおりです。

- Clang のデフォルトの C++ 標準は、**gnu++14** ではなく **gnu++17** になりました。
- **-Wimplicit-function-declaration**、**-Wimplicit-int**、および **-Wincomplicit-function-pointer-types** オプションは、C コードのデフォルトでエラーになるようになりました。これは、configure スクリプトの動作に影響を与える可能性があります。

デフォルトでは、Clang 16 は、GCC Toolset 13 によって提供される **libstdc++** ライブラリーバージョン 13 と **binutils 2.40** を使用します。

詳細は、LLVM リリースノート および Clang リリースノート を参照してください。

Bugzilla:2178806

Rust Toolset がバージョン 1.71.1 にリベース

Rust Toolset がバージョン 1.71.1 に更新されました。主な変更点は、以下のとおりです。

- パフォーマンスを向上させるための multiple producer, single consumer (mpsc) チャネルの新しい実装
- **crates.io** レジストリーをより効率的に使用するための新しい Cargo **sparse** インデックスプロトコル
- ワンタイム値の初期化のための新しい **OnceCell** および **OnceLock** タイプ
- Foreign Function Interface (FFI) 境界にまたがる強制アンワインドの使用を可能にする新しい **C-unwind** ABI 文字列

詳細は、一連のアップストリームリリース発表を参照してください。

- Announcing Rust 1.67.0
- Announcing Rust 1.68.0
- Announcing Rust 1.69.0
- Announcing Rust 1.70.0
- Announcing Rust 1.71.0

Bugzilla:2191740

Rust profiler_builtins ランタイムコンポーネントが利用可能になる

この機能拡張により、Rust **profile_builtins** ランタイムコンポーネントが利用できるようになりました。このランタイムコンポーネントは、次のコンパイラーオプションを有効にします。

-C instrument-coverage
: カバレッジプロファイリングを有効にします。

-C profile-generate
: プロファイルガイド付きの最適化を有効にします。

Bugzilla:2213875[1]

Go Toolset がバージョン 1.20.10 にリベース

Go Toolset がバージョン 1.20.10 に更新されました。

主な機能拡張は、次のとおりです。

- 内部表現に依存せずにスライスと文字列を処理するための新しい関数が **unsafe** パッケージに追加されました。
- 比較可能な型は、比較可能な制約を満たすことができるようになりました。
- 新しい **crypto/ecdh** パッケージ。
- **go build** および **go test** コマンドは、**-i** フラグを受け入れなくなりました。
- **go generate** および **go test** コマンドは、**-skip pattern** オプションを受け入れるようになりました。
- **go build**、**go install**、およびその他のビルド関連コマンドは、**-pgo** フラグと **-cover** フラグをサポートするようになりました。
- **go** コマンドは、C ツールチェーンのないシステムではデフォルトで **cgo** を無効にするようになりました。
- **go version -m** コマンドは、より多くの Go バイナリータイプの読み取りをサポートするようになりました。
- **go** コマンドは、C ツールチェーンのないシステムではデフォルトで **cgo** を無効にするようになりました。
- コードカバレッジプロファイルを単体テストからのみ収集するのではなく、アプリケーションと統合テストから収集するためのサポートが追加されました。

Bugzilla:2185260[1]

grafana がバージョン 9.2.10 にリベース

grafana パッケージがバージョン 9.2.10 に更新されました。主な変更点は、以下のとおりです。

- 時系列パネルがデフォルトの視覚化オプションになり、グラフパネルに置き換わりました。
- Grafana が新しい Prometheus および Loki クエリービルダーを提供します。
- Grafana に、複数の UI/UX およびパフォーマンスの改善が追加されました。
- ライセンスが Apache 2.0 から GNU Affero General Public License (AGPL) に変更されました。
- heatmap パネルは Grafana 全体で使用されるようになりました。
- Geomaps は距離と面積の両方を測定できるようになりました。
- Alertmanager は、**Prometheus Alertmanager** バージョン 0.24 に基づくようになりました。
- Grafana Alerting ルールは、実行エラーまたはタイムアウト時にデフォルトで **Error** 状態を返すようになりました。

- 式を公開ダッシュボードで使用できるようになりました。
- 結合変換で内部結合がサポートされるようになりました。
- パブリックダッシュボードで Grafana ダッシュボードを共有できるようになりました。
- 新しい Prometheus ストリーミングパーサーが、オプトイン機能として利用できるようになりました。

詳細は、アップストリームのリリースノートを参照してください。

- What's new in Grafana v8.0
- What's new in Grafana v9.0
- What's new in Grafana v9.1
- What's new in Grafana v9.2

Bugzilla:2193250

grafana-pcp がバージョン 5.1.1 にリベースされました。

Performance Co-Pilot Grafana プラグインを提供する **grafana-pcp** パッケージがバージョン 5.1.1 に更新されました。主な変更点は、以下のとおりです。

- クエリーエディター: レートの変換と時間使用率の変換を無効にするボタンを追加しました。
- Redis データソース:
  - 非推奨の **label_values(metric, label)** 関数を削除しました。
  - 多くの系列を持つメトリクスのネットワークエラーを修正しました (Performance Co-Pilot バージョン 6 以降が必要)。
- **pmproxy** API タイムアウトを 1 分に設定します。

Bugzilla:2193270

.NET 8.0 が利用可能になる

Red Hat Enterprise Linux 8.9 には .NET バージョン 8.0 が同梱されています。以下は、主な改善点です。

- C#12 および F#8 言語バージョンのサポートが追加されました。
- .NET ソフトウェア開発キットを直接使用してコンテナーイメージをビルドするためのサポートが追加されました。
- ガベージコレクター (GC)、Just-In-Time (JIT) コンパイラー、およびベースライブラリーのパフォーマンスが多くの点で向上しました。

Jira:RHELPLAN-164398[1]

4.10. IDENTITY MANAGEMENT

samba がバージョン 4.18.4 にリベース

samba パッケージはアップストリームバージョン 4.18.4 にアップグレードされ、以前のバージョンに対するバグ修正と拡張機能が提供されています。最も注目すべき変更点:

- 以前のリリースでのセキュリティーの向上は、メタデータの高いワークロードの Server Message Block (SMB) サーバーのパフォーマンスに影響を与えました。この更新により、このシナリオでのパフォーマンスが向上します。
- 新しい **wbinfo --change-secret-at=<domain_controller>** コマンドは、指定されたドメインコントローラーの信頼アカウントのパスワードの変更を強制します。
- デフォルトでは、Samba はアクセス制御リスト (ACL) をファイルの **security.NTACL** 拡張属性に保存します。**/etc/samba/smb.conf** ファイルの **acl_xattr:<security_acl_name>** 設定を使用して属性名をカスタマイズできるようになりました。カスタム拡張属性名は、**security.NTACL** のように保護された場所ではないことに注意してください。その結果、サーバーにローカルにアクセスできるユーザーはカスタム属性のコンテンツを変更し、ACL を侵害する可能性があります。

Samba 4.11 以降はサーバーメッセージブロックバージョン 1 (SMB1) プロトコルが非推奨となり、今後のリリースで削除されることに注意してください。

Samba を起動する前にデータベースファイルがバックアップされます。**smbd**、**nmbd**、または**winbind** サービスが起動すると、Samba が **tdb** データベースファイルを自動的に更新します。Red Hat は、**tdb** データベースファイルのダウングレードをサポートしていません。

Samba を更新した後、**testparm** ユーティリティーを使用して **/etc/samba/smb.conf** ファイルを確認します。

Bugzilla:2190417

ipa がバージョン 4.9.12 にリベース

ipa パッケージがバージョン 4.9.12 にアップグレードされました。詳細は、 アップストリームの FreeIPA のリリースノート を参照してください。

Bugzilla:2196425

複数の IdM グループとサービスを単一の Ansible タスクで管理できるようになる

ansible-freeipa のこの機能拡張により、単一の Ansible タスクを使用して、複数の Identity Management (IdM) ユーザーグループとサービスを追加、変更、削除できるようになりました。そのためには、**ipagroup** モジュールと **ipaservice** モジュールの **groups** と **services** オプションを使用します。

ipagroup で使用できる **groups** オプションを使用すると、特定のグループにのみ適用される複数のグループ変数を指定できます。このグループは、**name** 変数によって定義されます。これは、**groups** オプションの唯一の必須変数です。

同様に、**ipaservice** で使用できる **services** オプションを使用すると、特定のサービスにのみ適用される複数のサービス変数を指定できます。このサービスは、**name** 変数によって定義されます。これは、**services** オプションの唯一の必須変数です。

Jira:RHELDOCS-16474[1]

ansible-freeipa ipaserver ロールが Random Serial Numbers をサポートするようになる

この更新により、**ansible-freeipa ipaserver** ロールで **ipaserver_random_serial_numbers=true** オプションを使用できるようになりました。このようにして、Ansible を使用して Identity Management (IdM) サーバーをインストールするときに、PKI で証明書とリクエストの完全にランダムなシリアル番

号を生成できます。RSNv3 を使用すると、大規模な IdM インストールでの範囲管理を回避し、IdM を再インストールする際の一般的な競合を防ぐことができます。

重要

RSNv3 は、新しい IdM インストールでのみサポートされます。有効にした場合、すべての PKI サービスで RSNv3 を使用する必要があります。

Jira:RHELDOCS-16462[1]

ipaserver_remove_on_server オプションと ipaserver_ignore_topology_disconnect オプションが、ipaserver ロールで利用できるようになりました。

ipaserver ansible-freeipa ロールの **remove_server_from_domain** オプションを使用して、Identity Management (IdM) トポロジーからレプリカを削除すると、トポロジーが切断されます。ここで、ドメインの保持したい部分を指定する必要があります。具体的には、次のことを行う必要があります。

- **ipaserver_remove_on_server** 値を指定して、トポロジーのどの部分を保持するかを指定します。
- **ipaserver_ignore_topology_disconnect** を True に設定します。

remove_server_from_domain オプションを使用して IdM からレプリカを削除した場合に、接続されたトポロジーが保持される場合は、これらのオプションはどちらも必要ないことに注意してください。

Bugzilla:2127901

ipaclient ロールにより、IdM レベルでユーザーの subID 範囲を設定できるようになる

この更新により、**ipaclient** ロールには **ipaclient_subid** オプションが提供され、これを使用して Identity Management (IdM) レベルで subID 範囲を設定できるようになりました。新しいオプションを明示的に **true** に設定しないと、**ipaclient** ロールはデフォルトの動作を維持し、IdM ユーザーに設定された subID 範囲なしでクライアントをインストールします。

以前は、このロールは **sssd authselect** プロファイルを設定し、それによって **/etc/nsswitch.conf** ファイルがカスタマイズされていました。subID データベースは IdM を使用せず、**/etc/subuid** および **/etc/subgid** のローカルファイルのみに依存しました。

Bugzilla:2175766

ipacert Ansible モジュールを使用して IdM 証明書を管理できるようになる

ansible-freeipa ipacert モジュールを使用して、Identity Management (IdM) ユーザー、ホスト、およびサービスの SSL 証明書をリクエストまたは取得できるようになりました。ユーザー、ホスト、およびサービスは、これらの証明書を使用して IdM に対する認証を行うことができます。証明書を取り消したり、保留された証明書を復元したりすることもできます。

Bugzilla:2127906

MIT Kerberos が拡張 KDC MS-PAC 署名をサポートするようになる

この更新により、Red Hat が使用する MIT Kerberos は、最近の CVE に対応して Microsoft が導入した、2 種類の特権属性証明書 (PAC) 署名のうち 1 種類のサポートを実装します。具体的には、RHEL 8 の MIT Kerberos は、KB5020805 でリリースされ、CVE-2022-37967 に対処する拡張 KDC 署名をサポートします。

ABI の安定性の制約 のため、RHEL8 上の MIT Kerberos は、他の PAC 署名タイプ、つまり KB4598347 で定義されているチケット署名をサポートできないことに注意してください。

この機能拡張に関連する問題のトラブルシューティングについては、以下のナレッジベースの記事を参照してください。

- RHEL-8.9 IdM update, web UI and CLI 401 Unauthorized with KDC S4U2PROXY_EVIDENCE_TKT_WITHOUT_PAC - user and group objects need SIDs
- find_sid_for_ldap_entry - [file ipa_sidgen_cofind_sid_for_ldap_entry - [file ipa_sidgen_common.c, line 521]: Cannot convert Posix ID [120000023l] into an unused SID]
- When upgrading to RHEL9, IDM users are not able to login anymore
- POSIX IDs, SIDs and IDRanges in IPA

BZ#2211387 および BZ#2176406 も参照してください。

Bugzilla:2211390

RHEL 8.9 は 389-ds-base 1.4.3.37 を提供する

RHEL 8.9 は、**389-ds-base** パッケージのバージョン 1.4.3.37 とともに配布されます。

Bugzilla:2188628

新しい passwordAdminSkipInfoUpdate: on/off 設定オプションが利用可能になる

新しい **passwordAdminSkipInfoUpdate: on/off** 設定を **cn=config** エントリーに追加すると、パスワード管理者が実行するパスワード更新をきめ細かく制御できます。この設定を有効にすると、パスワードの更新で
は、**passwordHistory**、**passwordExpirationTime**、**passwordRetryCount**、**pwdReset**、および **passwdExpWarned** などの特定の属性は更新されません。

Bugzilla:2166332

4.11. グラフィックインフラストラクチャー

Intel Arc A シリーズグラフィックスが完全にサポートされるようになる

以前はテクノロジープレビューとして利用可能であった Intel Arc A-Series グラフィックス (Alchemist または DG2) 機能が完全にサポートされるようになりました。Intel Arc A-Series グラフィックスは、ハードウェアアクセラレーションを可能にする GPU で、主に PC ゲームで使用されます。

このリリースでは、**i915.force_probe** カーネルオプションを設定する必要がなくなり、これらの GPU の完全なサポートがデフォルトで有効になっています。

Bugzilla:2041686[1]

4.12. WEB コンソール

Podman ヘルスチェックアクションが利用可能になる

新しいコンテナーを作成するときに、次の Podman ヘルスチェックアクションのいずれかを選択できます。

- No action (デフォルト): アクションは実行しません。

- Restart: コンテナーを再起動します。
- Stop: コンテナーを停止します。
- Force stop: コンテナーを強制的に停止します。コンテナーが終了するのを待ちません。

Jira:RHELDOCS-16247[1]

Web コンソールのアカウントページの更新

この更新により、以下のように **Accounts** ページが更新されます。

- アカウント作成プロセス中にカスタムユーザー ID を追加し、ホームディレクトリーとシェルを定義できるようになりました。
- アカウントを作成するときに、パスワード検証により、キーの入力ごとにチェックがアクティブに実行されます。さらに、弱いパスワードには警告が表示されるようになりました。
- アカウントの詳細ページに、アカウントのホームディレクトリーとシェルが表示されるようになりました。
- アカウントの詳細ページからシェルを変更することが可能です。

Jira:RHELDOCS-16367[1]

4.13. RED HAT ENTERPRISE LINUX システムロール

postgresql RHEL システムロールが利用可能になる

新しい **postgresql** RHEL システムロールは、 **PostgreSQL** サーバーをインストール、設定、管理、起動します。このロールは、データベースサーバー設定を最適化してパフォーマンスを向上させます。

このロールは、RHEL 8 および RHEL 9 マネージドノード上で現在リリースされサポートされているバージョンの **PostgreSQL** をサポートします。

詳細は、postgresql RHEL システムロールを使用した PostgreSQL のインストールと設定を 参照してください。

Bugzilla:2151371

keylime_server RHEL システムロール

新しい **keylime_server** RHEL システムロールを使用すると、Ansible Playbook を使用して、RHEL 9 システム上の検証およびレジストラ Keylime コンポーネントを設定できます。Keylime は、Trusted Platform Module (TPM) テクノロジーを使用するリモートマシン証明ツールです。

Bugzilla:2224387

新しい ha_cluster システムロール機能のサポート

ha_cluster システムロールは、次の機能をサポートするようになりました。

- リソースおよびリソース操作のデフォルトの設定 (ルールを含む複数のデフォルトのセットを含む)。
- SBD watchdog カーネルモジュールのロードとブロック。これにより、インストールされているハードウェアウォッチドッグをクラスターで使用できるようになります。

- クラスターホストとクォーラムデバイスへの個別のパスワードの割り当て。これにより、同じクォーラムホストが複数の個別のクラスターに参加し、これらのクラスター上の **hacluster** ユーザーのパスワードが異なるデプロイメントを設定できます。

これらの機能を実装するために設定するパラメーターの詳細は、 **ha_cluster** RHEL システムロールを使用した高可用性クラスターの設定を 参照してください。

Bugzilla:2190483、Bugzilla:2190478、Bugzilla:2216485

storage システムのロールは、RAID LVM ボリュームのストライプサイズの設定をサポートする

この更新により、RAID LVM デバイスの作成時に、カスタムストライプサイズを指定できるようになりました。パフォーマンスを向上させるには、SAP HANA のカスタムストライプサイズを使用してください。RAID LVM ボリュームの推奨ストライプサイズは 64 KB です。

Bugzilla:2141961

podman RHEL システムロールが Quadlet、ヘルスチェック、シークレットをサポートするようになりました

Podman 4.6 以降では、**podman** RHEL システムロールで **podman_quadlet_specs** 変数を使用できるようになりました。Quadlet は、ユニットファイルを指定するか、インベントリー内で名前、ユニットのタイプ、仕様を指定して定義できます。ユニットのタイプは次のとおりです: **container**、**kube**、**network**、および **volume**。Quadlet は RHEL 8 上のルートコンテナーでのみ機能することに注意してください。Quadlet は、RHEL 9 上のルートレスコンテナーで動作します。

ヘルスチェックは、Quadlet コンテナータイプに対してのみサポートされます。**[Container]** セクションで、**HealthCmd** フィールドを指定して healthcheck コマンドを定義し、**HealthOnFailure** フィールドを指定してコンテナーが異常な場合のアクションを定義します。可能なオプションは、**none**、**kill**、**restart**、および **stop** です。

podman_secrets 変数を使用してシークレットを管理できます。詳細は、アップストリームのドキュメント を参照してください。

Jira:RHELPLAN-154440[1]

マウントポイントカスタマイズ用の新しいボリュームオプションが RHEL システムロールに追加される

この更新により、マウントディレクトリーに **mount_user**、**mount_group**、および **mount_permissions** パラメーターを指定できるようになりました。

Bugzilla:2181661

kdump RHEL システムロールの更新

kdump RHEL システムロールが新しいバージョンに更新され、次の主な機能拡張が行われました。

- **kexec-tools** をインストールすると、このファイルを管理する必要がなくなるため、ユーティリティースイートは **/etc/sysconfig/kdump** ファイルを生成しなくなります。
- このロールは、**auto_reset_crashkernel** 変数と **dracut_args** 変数をサポートしています。

詳細は、**/usr/share/doc/rhel-system-roles/kdump/** ディレクトリー内のリソースを参照してください。

Bugzilla:2211272

ad_integration RHEL システムロールが AD ドメインに再参加できるようになる

この更新により、**ad_integration** RHEL システムロールを使用して Active Directory (AD) ドメインに再参加できるようになりました。これを行うには、**ad_integration_force_rejoin** 変数を **true** に設定します。**realm_list** の出力で、ホストがすでに AD ドメインに存在していることが示されている場合、ホストは再参加する前に既存のドメインから離脱します。

Bugzilla:2211723

rhc システムロールがプロキシーサーバータイプの設定をサポートするようになる

rhc_proxy パラメーターの下に新しく導入された属性 **スキーム** により、**rhc** システムロールを使用してプロキシーサーバータイプを設定できるようになります。デフォルトの **http** と **https** の 2 つの値を設定できます。

Bugzilla:2211778

設定バックアップを無効にする ssh ロールの新しいオプション

新しい **ssh_backup** オプションを **false** に設定することで、古い設定ファイルが上書きされる前にバックアップされることを阻止できるようになりました。以前は、バックアップ設定ファイルが自動的に作成されていましたが、これは不要な場合がありました。**ssh_backup** オプションのデフォルト値は **true** で、元の動作が保持されます。

Bugzilla:2216759

certificate RHEL システムロールで、 certmonger の使用時に証明書ファイルモードを変更できるようになる

以前は、**certmonger** プロバイダーを使用して **certificate** RHEL システムロールによって作成された証明書で、デフォルトのファイルモードが使用されていました。ただし、ユースケースによっては、より制限のあるモードが必要になる場合があります。この更新により、**mode** パラメーターを使用して別の証明書とキーファイルモードを設定できるようになりました。

Bugzilla:2218204

systemd ユニットを管理するための新しい RHEL システムロール

rhel-system-role パッケージに **systemd** RHEL システムロールが含まれるようになりました。このロールを使用して、ユニットファイルをデプロイし、複数のシステム上で **systemd** ユニットを管理できます。**systemd** ユニットファイルとテンプレートを提供し、それらのユニットの状態 (開始、停止、マスクなど) を指定することで、**systemd** の機能を自動化できます。

Bugzilla:2224388

network RHEL システムロールは、 no-aaaa DNS オプションをサポートする

no-aaaa オプションを使用して、マネージドノードで DNS 設定を設定できるようになりました。以前は、**getaddrinfo** などの NSS ベースのインターフェイスによってトリガーされる AAAA ルックアップを含む、スタブリゾルバーによって生成される AAAA クエリーを抑制するオプションはありませんでした。DNS ルックアップのみが影響を受けていました。この機能拡張により、スタブリゾルバーによって生成された AAAA クエリーを抑制できるようになりました。

Bugzilla:2218595

network RHEL システムロールは、 DNS レコードの自動更新を制御する auto-dns オプションをサポートする

この機能拡張により、定義されたネームサーバーと検索ドメインのサポートが提供されます。DHCP か

らの **dns record** など、自動的に設定されたネームサーバーと検索ドメインを無効にしながら、**dns** および **dns_search** プロパティーで指定されたネームサーバーと検索ドメインのみを使用できるようになりました。この機能拡張により、**auto-dns** 設定を変更することで、自動 DNS 記録を自動的に無効にすることができます。

Bugzilla:2211273

firewall RHEL システムロールが、ipsets に関連する変数をサポートするようになる

firewall RHEL システムロールの今回の更新により、**ipsets** を定義、変更、削除できるようになりました。また、これらの **ipsets** をファイアウォールゾーンに追加したり、ファイアウォールゾーンから削除したりすることもできます。あるいは、ファイアウォールのリッチルールを定義するときに、これらの **ipsets** を使用することもできます。

次の変数を使用して、**firewall** RHEL システムロールで **ipsets** を管理できます。

- **ipset**
- **ipset_type**
- **ipset_entries**
- **short**
- **description**
- **state: present** または **state: absent**
- **permanent: true**

この機能拡張の主な利点は次のとおりです。

- 多くの IP アドレスのルールを定義するリッチルールの複雑さを軽減できます。
- 複数のルールを変更せずに、必要に応じてセットに IP アドレスを追加または削除できます。

詳細は、**/usr/share/doc/rhel-system-roles/firewall/** ディレクトリー内のリソースを参照してください。

Bugzilla:2140880

restorecon -T 0 による selinux システムロールのパフォーマンスの向上

selinux システムロールは、該当するすべてのケースで、**restorecon** コマンドで **-T 0** オプションを使用するようになりました。これにより、ファイル上でデフォルトの SELinux セキュリティーコンテキストを復元するタスクのパフォーマンスが向上します。

Bugzilla:2192343

firewall RHEL システムロールに競合するサービスを無効にするオプションが追加され、firewalld がマスクされている場合でもロールが失敗しなくなる

以前は、ロールの実行時に **firewalld** サービスがマスクされていた場合、または競合するサービスが存在した場合に、**firewall** システムロールは失敗していました。この更新では、次の 2 つの主な機能拡張が提供されます。

linux-system-roles.firewall ロールは、ロールの実行時に常に **firewalld** サービスのインストール、マスク解除、および有効化を試みます。新しい変数 **firewall_disable_conflicting_services** を Playbook

に追加して、競合する既知のサービス (**iptables.service**、**nftables.service**、**ufw.service** など) を無効化できるようになりました。**firewall_disable_conflicting_services** 変数はデフォルトで **false** に設定されます。競合するサービスを無効にするには、変数を **true** に設定します。

Bugzilla:2222809

podman RHEL システムロールは、getsubids を使用してサブ ID とサブ ID を取得するようになりました。

podman RHEL システムロールは、**getsubids** コマンドを使用して、ユーザーとグループの subuid と subgid の範囲をそれぞれ取得するようになりました。**podman** RHEL システムロールもこのコマンドを使用して、アイデンティティー管理で動作するユーザーとグループを確認します。

Jira:RHEL-866[1]

podman_kube_specs 変数が pull_image と continue_if_pull_fails フィールドをサポートするようになりました。

podman_kube_specs 変数が新しいフィールドをサポートするようになりました。

- **pull_image**: 使用前にイメージがプルされるようにします。デフォルト値は **true** です。イメージがシステム上に存在することを確認するメカニズムが他にあり、イメージをプルしない場合は、**false** を使用してください。
- **continue_if_pull_fails**: イメージのプルが失敗しても、致命的なエラーとして扱わず、ロールを使用して続行します。デフォルトは **false** です。正しいイメージがシステム上に存在することを確認するメカニズムが他にある場合は、**true** を使用します。

Jira:RHEL-858[1]

firewall RHEL システムロール設定をリセットしたときに、ダウンタイムが最小限で済むようになる

以前は、**previous: replace** 変数を使用して **firewall** ロール設定をリセットすると、**firewalld** サービスが再起動されました。再起動するとダウンタイムが追加され、**firewalld** がアクティブな接続からのトラフィックをブロックしないオープン接続の期間が長くなります。この機能拡張により、**firewalld** サービスは再起動ではなく再ロードすることで、設定のリセットを完了します。リロードによりダウンタイムが最小限に抑えられ、ファイアウォールルールをバイパスする機会が減ります。その結果、**以前の: replace** 変数を使用して **firewall** ロール設定をリセットすると、ダウンタイムが最小限で済むようになりました。

Bugzilla:2224648

4.14. クラウド環境の RHEL

cloud-init は、NetworkManager キーファイルをサポートする

この更新により、**cloud-init** ユーティリティーは NetworkManager (NM) キーファイルを使用して、作成されたクラウドインスタンスのネットワークを設定できるようになりました。

デフォルトでは、**cloud-init** は、依然としてネットワークセットアップに **sysconfig** メソッドを使用することに注意してください。代わりに NM キーファイルを使用するように **cloud-init** を設定するには、**/etc/cloud/cloud.cfg** を編集し、**network-manager** をプライマリーネットワークレンダラーとして設定します。

```
# cat /etc/cloud/cloud.cfg
```

```
network:
  renderers: ['network-manager', 'eni', 'netplan', 'sysconfig', 'networkd']
```

Bugzilla:2219528[1]

cloud-init が ESXi 上でデフォルトで VMware データソースを使用するようになる

VMware vSphere クラウドプラットフォームなどの VMware ESXi ハイパーバイザーを使用するホスト上に RHEL 仮想マシン (VM) を作成する場合。これにより、**cloud-init** を使用して RHEL の ESXi インスタンスを作成する際のパフォーマンスと安定性が向上します。ただし、ESXi は Open Virtualization Format (OVF) データソースと引き続き互換性があり、VMware のデータソースが使用できない場合でも OVF データソースを使用できる点に留意してください。

Bugzilla:2230777[1]

4.15. サポート性

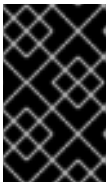
sos がバージョン 4.6 にリベース

設定、診断、およびトラブルシューティングデータを収集するための **sos** ユーティリティーが、バージョン 4.6 にリベースされました。この更新では、次の機能拡張が提供されます。

- **sos** レポートには、起動に関する問題のトラブルシューティングに重要な情報が含まれる可能性がある **/boot/grub2/custom.cfg** ファイルと **/boot/grub2/user.cfg** ファイルの両方の内容が含まれるようになりました。(BZ#2213951)
- OVN-Kubernetes の **sos** プラグインは、相互接続環境の追加のログを収集します。今回の更新により、**ovnkube-node** および **ovnkube-controller** の両方のコンテナーが 1 つにマージされるときに、**sos** は **ovnkube-controller** コンテナーからもログを収集します。

さらに、注目すべきバグ修正には以下が含まれます。

- **sos** は、OpenShift Container Platform 4 環境で **cgroup** データを正しく収集するようになりました (BZ#2186361)。
- **sudo** プラグインを有効にして **sos** レポートを収集しているときに、**sos** は **bindpw** オプションを適切に削除するようになりました。(BZ#2143272)
- **subscription_manager** プラグインは、**/var/lib/rhsm/** パスからプロキシーのユーザー名とパスワードを収集しなくなりました。(BZ#2177282)
- **virsh** プラグインは、virt-manager ログ内の SPICE リモートディスプレイパスワードを収集しなくなりました。これにより、**sos** がレポートでパスワードを開示できなくなります。(BZ#2184062)
- **sos** は、**/var/lib/iscsi/nodes/<IQN>/<PortalIP>/default** ファイルに以前に表示されていたユーザー名とパスワードをマスクするようになりました。



重要

生成されたアーカイブには、機密とみなされるデータが含まれる可能性があります。したがって、アーカイブを第三者に渡す前に必ず内容を確認する必要があります。

(BZ#2187859)

- **sos** は、ログファイルのサイズが超過した場合やプラグインがタイムアウトした場合でも、テールログ収集を完了します。(BZ#2203141)
- Pacemaker クラスターノードで **soscollect** コマンドを入力すると、**sos** は、同じクラスターノードから sos レポートを収集します。(BZ#2186460)
- OpenShift Container Platform 4 環境のホストからデータを収集する場合、**sos** は **sysroot** パスを使用するようになり、正しいデータのみがアセンブルされるようになります。(BZ#2075720)
- **sos report --clean** コマンドは、意図したとおりにすべての MAC アドレスを難読化します。(BZ#2207562)
- **hpssm** プラグインを無効にしても例外は発生しなくなりました。(BZ#2216608)
- **sos clean** コマンドは、サニタイズされたファイルのパーミッションに従います。(BZ#2218279)

sos の各リリースの詳細は、アップストリームのリリースノート を参照してください。

Jira:RHELPLAN-156196[1]

4.16. コンテナー

Podman は、zstd で圧縮されたイメージのプルとプッシュをサポートする

zstd 形式で圧縮されたイメージをプルおよびプッシュできます。zstd 圧縮は、gzip よりも効率的で高速です。イメージのプルとプッシュに関連するネットワークトラフィックとストレージの量を削減できます。

Jira:RHELPLAN-154313[1]

Podman の Quadlet が利用可能になる

Podman v4.6 以降では、Quadlet を使用して、コンテナーの説明から **systemd** サービスファイルを自動的に生成できます。Quadlets は、関連するコンテナーの詳細に焦点を当てて説明しており、**systemd** でコンテナーを実行するという技術的な複雑さを考慮していないため、**podman generate systemd** コマンドよりも使いやすい可能性があります。なお、Quadlet はルートフルコンテナーでのみ機能します。

詳細は、Quadlet upstream documentation および Make systemd better for Podman with Quadlet の記事を参照してください。

Jira:RHELPLAN-154431[1]

Container Tools パッケージが更新される

Podman、Buildah、Skopeo、crun、runc ツールを含む、更新された Container Tools パッケージが利用可能になりました。この更新では、以前のバージョンに対する一連のバグ修正と機能拡張が適用されます。

Podman v4.6 の注目すべき変更点は次のとおりです。

- **podman kube play** コマンドは、Pod のコンテナー内で使用される環境変数を Kubernetes YAML ファイルに提供する **--configmap=<path>** オプションをサポートするようになりました。
- **podman kube play** コマンドは、**--configmap** オプション用の複数の Kubernetes YAML ファイルをサポートするようになりました。
- **podman kube play** コマンドは、liveness プローブ内の containerPort 名とポート番号をサポートするようになりました。
- **podman kube play** コマンドは、ctrName をエイリアスとして Pod ネットワークに追加するようになりました。
- **podman kube play** および **podman kube generated** コマンドは、SELinux ファイルタイプラベルと ulimit アノテーションをサポートするようになりました。
- 指定された名前のシークレットが存在するかを検証する、新しいコマンド **podman secret exists** が追加されました。
- **podman create**、**podman run**、**podman pod create**、および **podman pod clone** コマンドは、新しいオプション **--shm-size-systemd** をサポートするようになりました。これにより、systemd 固有のマウントの tmpfs サイズを制限できるようになります。
- **podman create** および podman run コマンドは、新しいオプション **--security-opt label=nested** をサポートするようになりました。これにより、制限されたコンテナー内で SELinux のラベル付けが可能になります。
- Podman は、Pod 内で実行されているコンテナーの自動更新をサポートするようになりました。
- Podman は、安定性を高めるために SQLite データベースをバックエンドとして使用できるようになりました。デフォルトは BoltDB データベースのままです。データベースを選択するには、**containers.conf** ファイルの **database_backend** フィールドを設定します。
- Podman は、コンテナーの説明から **systemd** サービスファイルを自動的に生成する Quadlets をサポートするようになりました。この説明では、関連するコンテナーの詳細に焦点を当てており、**systemd** でコンテナーを実行する際の技術的な複雑さは隠しています。

注目すべき変更点の詳細は、アップストリームのリリースノート を参照してください。

Jira:RHELPLAN-154443[1]

Podman が Podmansh ログインシェルをサポートするようになる

Podman v4.6 以降、**Podmansh** ログインシェルを使用して、ユーザーアクセスと制御を管理できるようになりました。CGroups v2 に切り替えるには、**systemd.unified_cgroup_hierarchy=1** をカーネルコマンドラインに追加します。標準のシェルコマンド (**/usr/bin/bash** など) の代わりに、ログインシェルとして **/usr/bin/podmansh** コマンドを使用するようにユーザーの設定を行います。ユーザーがシステムセットアップにログインすると、**podmansh** コマンドはユーザーのセッションを **podmansh** という名前の Podman コンテナー内で実行します。ユーザーがログインするコンテナーは、**/etc/containers/systemd/users/** ディレクトリーに作成される Quadlet ファイルを使用して定義されます。これらのファイルで、**[Container]** セクションの **ContainerName** フィールドを **podmansh** に設定します。systemd は、ユーザーセッションの開始時に **podmansh** を自動的に起動し、すべてのユーザーセッションが終了するまで実行を続けます。

詳細は、Podman v4.6.0 Introduces Podmansh: A Revolutionary Login Shell を参照してください。

Jira:RHELPLAN-163002[1]

Fulcio および Rekor を使用した sigstore 署名のクライアントが利用可能になる

Fulcio および Rekor サーバーを使用すると、秘密鍵を手動で管理する代わりに、OpenID Connect (OIDC) サーバー認証に基づく短期証明書を使用して署名を作成できるようになりました。以前はテクノロジープレビューとして利用可能であった、Fulcio および Rekor を使用した sigstore 署名のクライアントが、完全にサポートされるようになりました。この追加機能はクライアント側のサポートのみであり、Fulcio サーバーや Rekor サーバーは含まれません。

policy.json ファイルに **fulcio** セクションを追加します。コンテナーイメージに署名するには、**podman push --sign-by-sigstore=file.yml** または **skopeo copy --sign-by-sigstore=file.yml** コマンドを使用します。ここで、**file.yml** は sigstore 署名パラメーターファイルです。

署名を検証するには、**policy.json** ファイルに **fulcio** セクションと **rekorPublicKeyPath** または **rekorPublicKeyData** フィールドを追加します。詳細は、**containers-policy.json** の man ページを参照してください。

Jira:RHELPLAN-160659[1]

第5章 外部カーネルパラメーターへの重要な変更

本章では、システム管理者向けに、Red Hat Enterprise Linux 8.9 に同梱されるカーネルにおける重要な変更の概要について説明します。変更には、たとえば、**proc** エントリー、**sysctl** および **sysfs** のデフォルト値、ブートパラメーター、カーネル設定オプション、または重要な動作の変更などが含まれます。

新しいカーネルパラメーター

gather_data_sampling=[X86,INTEL]

このカーネルパラメーターを使用すると、Gather Data Sampling (GDS) の軽減策を制御できます。GDS は、ベクトルレジスターに以前に格納されていたデータへの特権のない投機的アクセスを許可するハードウェアの脆弱性です。

この問題は、更新されたマイクロコードではデフォルトで軽減されています。軽減策はパフォーマンスに影響を与える可能性がありますが、無効にすることができます。マイクロコード軽減策のないシステムが、軽減策として AVX を無効にしています。利用可能な値は次のとおりです。

- **force** - AVX を無効にして、マイクロコード軽減策を使用せずにシステムを軽減します。マイクロコード軽減策が存在する場合は効果がありません。バグのある AVX 列挙によりユーザー空間でクラッシュが発生することが知られています。
- **off** - GDS 軽減策を無効化します。

rdrand=[X86]

このカーネルパラメーターを使用すると、RDRAND サポートのアドバタイズメントを非表示にすることができます。このパラメーターは、BIOS サポート、特にサスペンドまたはレジュームパス周りにバグがあるため、特定の AMD プロセッサーに影響します。

- **force**: RDRAND サポートのアドバタイズメントを非表示にするカーネルによる決定をオーバーライドします。

更新されたカーネルパラメーター

intel_pstate=[X86]

このカーネルパラメーターを CPU パフォーマンスのスケーリングに使用できます。利用可能な値は次のとおりです。

- **disable** - サポートされているプロセッサーのデフォルトのスケーリングドライバーとして **intel_pstate** を有効にしないでください。
- **[新規] active** - **intel_pstate** ドライバーを使用して、**cpufreq** のスケーリングガバナー層をバイパスし、p-state 選択用の独自のアルゴリズムを提供します。アクティブモードで **intel_pstate** によって提供される P-state 選択アルゴリズムには、powersave と performance の 2 つがあります。両方の動作方法は、プロセッサーで、そして場合によってはプロセッサーモデルで、ハードウェア管理 P-state (HWP) 機能が有効になっているかどうかによって異なります。
- **パッシブ** - **intel_pstate を** スケーリングドライバーとして使用しますが、(内部ガバナーを有効にするのではなく) 汎用の **cpufreq** ガバナーと連携して動作するように設定します。このモードは、ハードウェア管理の P-state (HWP) 機能と一緒に使用することはできません。
- **force** - **acpi-cpufreq** を優先して **intel_pstate** をデフォルトで禁止しているシステムで、これを有効化します。**acpi-cpufreq** の代わりに **intel_pstate** ドライバーを強制すると、OSPM に示される ACPI P-States 情報に依存するプラットフォーム機能 (温度制御や電力制

限など) が無効になる可能性があるため、注意して使用する必要があります。このオプションは、**intel_pstate** ドライバーでサポートされていないプロセッサーや、**acpi-cpufreq** の代わりに **pcc-cpufreq** を使用するプラットフォームでは機能しません。

- **no_hwp** - ハードウェア P ステートコントロール (HWP) が利用可能な場合は有効にしません。
- **hwp_only** - ハードウェア P state コントロール (HWP) が利用可能な場合は、それをサポートするシステムにのみ **intel_pstate** をロードします。
- **support_acpi_ppc** - **ACPI _PPC** パフォーマンス制限を強制します。Fixed ACPI Description Table で優先電源管理プロファイルを "エンタープライズサーバー" または "パフォーマンスサーバー" として指定している場合、この機能はデフォルトでオンになります。
- **per_cpu_perf_limits** - **cpufreq sysfs** インターフェイスを使用して、論理 CPU ごとの P-State パフォーマンス制御の制限を許可します。

rdt=[HW,X86,RDT]

このカーネルパラメーターを使用すると、個々の RDT 機能をオンまたはオフにすることができます。リストには、**cmt**、**mbmtotal**、**mbmlocal**、**l3cat**、**l3cdp**、**l2cat**、**l2cdp**、**mba**、**[新規] smba**、**[新規] bmec** を含めます。
たとえば、**cmt** をオンにして **mba** をオフにするには、次を使用します。

```
rdt=cmt,!mba
```

tsc=[x86]

このカーネルパラメーターを使用すると、TSC のクロックソース安定性チェックを無効にすることができます。このパラメーターの形式は **<string>** です。

- **reliable**: tsc クロックソースを信頼できるものとしてマークします。これにより、起動時の安定性チェックだけでなく、実行時のクロックソース検証も無効になります。古いハードウェアおよび仮想化環境で高分解能タイマーモードを有効にするために使用されます。
- **noirqtime**: TSC を使用して **irq** アカウンティングを実行しません。RDTSC が遅れており、この計算によってオーバーヘッドが追加される可能性があるプラットフォームで、実行時に **IRQ_TIME_ACCOUNTING** を無効にするために使用されます。
- **unstable**: TSC クロックソースを不安定としてマークします。起動時に TSC を無条件に不安定としてマークし、TSC ウォッチドッグが認識した後のそれ以上の揺らぎを回避します。
- **nowatchdog**: クロックソースウォッチドッグを無効にします。レイテンシー要件が厳しい状況 (クロックソースウォッチドッグからの割り込みが許容されない場合) で使用されます。
- **recalibrate**: MSR または CPUID(0x15) を使用して TSC 周波数が HW または FW から取得されるシステム上で、HW タイマー (HPET または PM タイマー) に対する再キャリブレーションを強制します。差が 500 ppm を超える場合は警告します。

新しい sysctl パラメーター

nmi_wd_lpm_factor=(PPC only)

NMI ウォッチドッグタイムアウトに適用する係数 (**nmi_watchdog** が **1** に設定されている場合のみ)。この係数は、LPM 中に NMI ウォッチドッグタイムアウトを計算するときに **watchdog_thresh**

に追加されるパーセンテージを表します。ソフトロックアップのタイムアウトは影響を受けません。

- 値 **0** は変化がないことを意味します。
- デフォルト値は **200** です。これは、NMI ウォッチドッグが 30 秒に設定されることを意味します (**watchdog_thresh** が 10 に等しいことに基づく)。

txrehash

このカーネルパラメーターを使用すると、ソケットでのデフォルトのハッシュ再考動作を制御できます。

- **1** (デフォルト) に設定すると、リスニングソケットでハッシュの再考が実行されます。
- **0** に設定すると、ハッシュの再考は実行されません。

第6章 デバイスドライバー

6.1. 新しいドライバー

ネットワークドライバー

- Thunderbolt/USB4 ネットワークドライバー (**thunderbolt_net**)
- Broadcom 802.11 ワイヤレス LAN fullmac ドライバー (**brcmfmac**) (64 ビット ARM アーキテクチャーのみ)

グラフィックドライバーとその他のドライバー

- MediaTek デバイスバージョン 0.1 (**btmtk**) の Bluetooth サポート (IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)
- DRM Buddy Allocator (**drm_buddy**) (64 ビット IBM Z アーキテクチャーのみ)
- DRM ディスプレイアダプターヘルパー (**drm_display_helper**) (64 ビット IBM Z アーキテクチャーのみ)
- Microsoft Azure Network Adapter IB ドライバー (**mana_ib**) (AMD および Intel 64 ビットアーキテクチャーのみ)
- Linux USB Video Class ドライバー (**uvc**) (IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)
- Intel Meteor Lake PCH pinctrl/GPIO ドライバー (**pinctrl-meteorlake**) (AMD および Intel 64 ビットアーキテクチャーのみ)
- Intel In Field Scan (IFS) デバイス (**intel_ifs**) (AMD および Intel 64 ビットアーキテクチャーのみ)
- Intel Uncore Frequency Common Module (**intel-uncore-frequency-common**)、AMD および Intel 64 ビットアーキテクチャーのみ
- Intel Uncore Frequency Limits Driver (**intel-uncore-frequency**)、AMD および Intel 64 ビットアーキテクチャーのみ
- AMD SoundWire ドライバー (**soundwire-amd**) (AMD および Intel 64 ビットアーキテクチャーのみ)
- DisplayPort Alternate Mode (**typec_displayport**)、64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ
- Virtio-mem ドライバー (**virtio_mem**)、AMD および Intel 64 ビットアーキテクチャーのみ

6.2. 更新されたドライバー

ネットワークドライバーの更新

- Realtek RTL8152/RTL8153 ベースの USB イーサネットアダプター (**r8152**) がバージョン v1.12.13 に更新されました (64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)。

次のドライバーが **カーネルバージョン 4.18.0-513.5.1** に更新されました。

- Intel® 10 Gigabit PCI Express Network Driver (**ixgbe**)、64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ
- Intel® 10 Gigabit Virtual Function Network Driver (**ixgbevf**)、64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ
- Intel® 2.5G Ethernet Linux Driver (**igc**)、64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ
- Intel® Ethernet Adaptive Virtual Function Network Driver (**iavf**)、64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ
- Intel® Ethernet Connection XL710 Network Driver (**i40e**)、64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ
- Intel® Ethernet Switch Host Interface Driver (**fm10k**)、64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ
- Intel® Gigabit Ethernet Network Driver (**igb**)、64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ
- Intel® Gigabit Virtual Function Network Driver (**igbvf**)、64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ
- Intel® PRO/1000 Network Driver (**e1000e**)、64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ
- Mellanox 第 5 世代ネットワークアダプター (ConnectX シリーズ) コアドライバー (**mlx5_core**)
- Netronome Flow Processor (NFP) ドライバー (**nfp**)

グラフィックス、ストレージ、その他のドライバーの更新

- Broadcom MegaRAID SAS Driver (**megaraid_sas**) がバージョン 07.725.01.00-rc1 に更新されました (64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)。
- Driver for Microchip Smart Family Controller (**smartpqi**) がバージョン 2.1.22-040 に更新されました (64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)。
- Emulex LightPulse Fibre Channel SCSI ドライバー (**lpfc**) がバージョン 0:14.0.0.21 に更新されました (64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)。
- MPI3 Storage Controller Device Driver (**mpi3mr**) がバージョン 8.4.1.0.0 に更新されました (64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)。
- QLogic Fibre Channel HBA Driver (**qla2xxx**) がバージョン 10.02.08.200-k に更新されました (64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)。

第7章 利用可能な BPF 機能

この章では、Red Hat Enterprise Linux 8 のこのマイナーバージョンのカーネルで利用可能な **Berkeley Packet Filter** (**BPF**) 機能の完全なリストを提供します。表には次のリストが含まれます。

- システム設定とその他のオプション
- 利用可能なプログラムの種類とサポートされているヘルパー
- 利用可能なマップの種類

この章には、**bpftool feature** コマンドの自動生成された出力が含まれています。

表7.1 システム設定とその他のオプション

オプション	値
unprivileged_bpf_disabled	1 (特権ユーザーに限定された bpf() syscall、リカバリーなし)
JIT コンパイラー	1 (有効)
JIT コンパイラーの強化	1 (権限のないユーザーに対して有効)
JIT コンパイラー kallsyms エクスポート	1 (ルートで有効)
非特権ユーザーの JIT のメモリー制限	264241152
CONFIG_BPF	y
CONFIG_BPF_SYSCALL	y
CONFIG_HAVE_EBPF_JIT	y
CONFIG_BPF_JIT	y
CONFIG_BPF_JIT_ALWAYS_ON	y
CONFIG_DEBUG_INFO_BTF	y
CONFIG_DEBUG_INFO_BTF_MODULES	n
CONFIG_CGROUPS	y
CONFIG_CGROUP_BPF	y
CONFIG_CGROUP_NET_CLASSID	y
CONFIG_SOCK_CGROUP_DATA	y

オプション	値
CONFIG_BPF_EVENTS	y
CONFIG_KPROBE_EVENTS	y
CONFIG_UPROBE_EVENTS	y
CONFIG_TRACING	y
CONFIG_FTRACE_SYSCALLS	y
CONFIG_FUNCTION_ERROR_INJECTION	y
CONFIG_BPF_KPROBE_OVERRIDE	y
CONFIG_NET	y
CONFIG_XDP_SOCKETS	y
CONFIG_LWTUNNEL_BPF	y
CONFIG_NET_ACT_BPF	m
CONFIG_NET_CLS_BPF	m
CONFIG_NET_CLS_ACT	y
CONFIG_NET_SCH_INGRESS	m
CONFIG_XFRM	y
CONFIG_IP_ROUTE_CLASSID	y
CONFIG_IPV6_SEG6_BPF	n
CONFIG_BPF_LIRC_MODE2	n
CONFIG_BPF_STREAM_PARSER	y
CONFIG_NETFILTER_XT_MATCH_BPF	m
CONFIG_BPFILTER	n
CONFIG_BPFILTER_UMH	n

オプション	値
CONFIG_TEST_BPF	m
CONFIG_HZ	1000
bpf() syscall	available
大きなプログラムサイズの制限	available

表7.2 利用可能なプログラムの種類とサポートされているヘルパー

プログラムの種類	利用可能なヘルパー
socket_filter	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_perf_event_output, bpf_skb_load_bytes, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_skb_load_bytes_relative, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
kprobe	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_override_return, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf

プログラムの種類	利用可能なヘルパー
sched_cls	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_l3_csum_replace, bpf_l4_csum_replace, bpf_tail_call, bpf_clone_redirect, bpf_get_cgroup_classid, bpf_skb_vlan_push, bpf_skb_vlan_pop, bpf_skb_get_tunnel_key, bpf_skb_set_tunnel_key, bpf_redirect, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_get_tunnel_opt, bpf_skb_set_tunnel_opt, bpf_skb_change_proto, bpf_skb_change_type, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_change_tail, bpf_skb_pull_data, bpf_csum_update, bpf_set_hash_invalid, bpf_get_numa_node_id, bpf_skb_change_head, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_set_hash, bpf_skb_adjust_room, bpf_skb_get_xfrm_state, bpf_skb_load_bytes_relative, bpf_fib_lookup, bpf_skb_cgroup_id, bpf_skb_ancestor_cgroup_id, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sk_fullsock, bpf_tcp_sock, bpf_skb_ecn_set_ce, bpf_get_listener_sock, bpf_skc_lookup_tcp, bpf_tcp_check_syncookie, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_tcp_gen_syncookie, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_sk_assign, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_csum_level, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_skb_cgroup_classid, bpf_redirect_neigh, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_redirect_peer, bpf_ktime_get_coarse_ns, bpf_check_mtu, bpf_for_each_map_elem, bpf_snprintf
sched_act	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_l3_csum_replace, bpf_l4_csum_replace, bpf_tail_call, bpf_clone_redirect, bpf_get_cgroup_classid, bpf_skb_vlan_push, bpf_skb_vlan_pop, bpf_skb_get_tunnel_key, bpf_skb_set_tunnel_key, bpf_redirect, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_get_tunnel_opt, bpf_skb_set_tunnel_opt, bpf_skb_change_proto, bpf_skb_change_type, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_change_tail, bpf_skb_pull_data, bpf_csum_update, bpf_set_hash_invalid, bpf_get_numa_node_id, bpf_skb_change_head, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_set_hash, bpf_skb_adjust_room, bpf_skb_get_xfrm_state, bpf_skb_load_bytes_relative, bpf_fib_lookup, bpf_skb_cgroup_id, bpf_skb_ancestor_cgroup_id, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sk_fullsock, bpf_tcp_sock, bpf_skb_ecn_set_ce, bpf_get_listener_sock, bpf_skc_lookup_tcp, bpf_tcp_check_syncookie, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_tcp_gen_syncookie, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_sk_assign, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_csum_level, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_skb_cgroup_classid, bpf_redirect_neigh, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_redirect_peer, bpf_ktime_get_coarse_ns, bpf_check_mtu, bpf_for_each_map_elem, bpf_snprintf

プログラムの種類	利用可能なヘルパー
tracepoint	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
xdp	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_redirect, bpf_perf_event_output, bpf_csum_diff, bpf_get_current_task, bpf_get_numa_node_id, bpf_xdp_adjust_head, bpf_redirect_map, bpf_xdp_adjust_meta, bpf_xdp_adjust_tail, bpf_fib_lookup, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_skc_lookup_tcp, bpf_tcp_check_syncookie, bpf_tcp_gen_syncookie, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_check_mtu, bpf_for_each_map_elem, bpf_snprintf
perf_event	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_perf_prog_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_read_branch_records, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf

プログラムの種類	利用可能なヘルパー
cgroup_skb	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_perf_event_output, bpf_skb_load_bytes, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_skb_load_bytes_relative, bpf_skb_cgroup_id, bpf_get_local_storage, bpf_skb_ancestor_cgroup_id, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sk_fullsock, bpf_tcp_sock, bpf_skb_ecn_set_ce, bpf_get_listener_sock, bpf_skc_lookup_tcp, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_sk_cgroup_id, bpf_sk_ancestor_cgroup_id, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
cgroup_sock	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_get_cgroup_classid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sk_storage_get, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_netns_cookie, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
lwt_in	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_cgroup_classid, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_pull_data, bpf_get_numa_node_id, bpf_lwt_push_encap, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf

プログラムの種類	利用可能なヘルパー
lwt_out	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_cgroup_classid, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_pull_data, bpf_get_numa_node_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
lwt_xmit	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_l3_csum_replace, bpf_l4_csum_replace, bpf_tail_call, bpf_clone_redirect, bpf_get_cgroup_classid, bpf_skb_get_tunnel_key, bpf_skb_set_tunnel_key, bpf_redirect, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_get_tunnel_opt, bpf_skb_set_tunnel_opt, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_change_tail, bpf_skb_pull_data, bpf_csum_update, bpf_set_hash_invalid, bpf_get_numa_node_id, bpf_skb_change_head, bpf_lwt_push_encap, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_csum_level, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
sock_ops	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_setsockopt, bpf_sock_map_update, bpf_getsockopt, bpf_sock_ops_cb_flags_set, bpf_sock_hash_update, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_tcp_sock, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_load_hdr_opt, bpf_store_hdr_opt, bpf_reserve_hdr_opt, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf

プログラムの種類	利用可能なヘルパー
sk_skb	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_tail_call, bpf_perf_event_output, bpf_skb_load_bytes, bpf_get_current_task, bpf_skb_change_tail, bpf_skb_pull_data, bpf_get_numa_node_id, bpf_skb_change_head, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_skb_adjust_room, bpf_sk_redirect_map, bpf_sk_redirect_hash, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_skc_lookup_tcp, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
cgroup_device	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_uid_gid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
sk_msg	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_cgroup_classid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_msg_redirect_map, bpf_msg_apply_bytes, bpf_msg_cork_bytes, bpf_msg_pull_data, bpf_msg_redirect_hash, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_msg_push_data, bpf_msg_pop_data, bpf_spin_lock, bpf_spin_unlock, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf

プログラムの種類	利用可能なヘルパー
raw_tracepoint	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
cgroup_sock_addr	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_get_cgroup_classid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_setsockopt, bpf_getsockopt, bpf_bind, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_skc_lookup_tcp, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_netns_cookie, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
lwt_seg6local	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_cgroup_classid, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_pull_data, bpf_get_numa_node_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
lirc_mode2	サポート対象外

プログラムの種類	利用可能なヘルパー
sk_reuseport	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_skb_load_bytes, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_skb_load_bytes_relative, bpf_sk_select_reuseport, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
flow_dissector	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_skb_load_bytes, bpf_get_current_task, bpf_get_numa_node_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
cgroup_sysctl	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_uid_gid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sysctl_get_name, bpf_sysctl_get_current_value, bpf_sysctl_get_new_value, bpf_sysctl_set_new_value, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
raw_tracepoint_writable	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf

プログラムの種類	利用可能なヘルパー
cgroup_sockopt	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_uid_gid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_tcp_sock, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
tracing	サポート対象外

プログラムの種類	利用可能なヘルパー
struct_ops	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_l3_csum_replace, bpf_l4_csum_replace, bpf_tail_call, bpf_clone_redirect, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_get_cgroup_classid, bpf_skb_vlan_push, bpf_skb_vlan_pop, bpf_skb_get_tunnel_key, bpf_skb_set_tunnel_key, bpf_perf_event_read, bpf_redirect, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_get_stackid, bpf_csum_diff, bpf_skb_get_tunnel_opt, bpf_skb_set_tunnel_opt, bpf_skb_change_proto, bpf_skb_change_type, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_skb_change_tail, bpf_skb_pull_data, bpf_csum_update, bpf_set_hash_invalid, bpf_get_numa_node_id, bpf_skb_change_head, bpf_xdp_adjust_head, bpf_probe_read_str, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_set_hash, bpf_setsockopt, bpf_skb_adjust_room, bpf_redirect_map, bpf_sk_redirect_map, bpf_sock_map_update, bpf_xdp_adjust_meta, bpf_perf_event_read_value, bpf_perf_prog_read_value, bpf_getsockopt, bpf_override_return, bpf_sock_ops_cb_flags_set, bpf_msg_redirect_map, bpf_msg_apply_bytes, bpf_msg_cork_bytes, bpf_msg_pull_data, bpf_bind, bpf_xdp_adjust_tail, bpf_skb_get_xfrm_state, bpf_get_stack, bpf_skb_load_bytes_relative, bpf_fib_lookup, bpf_sock_hash_update, bpf_msg_redirect_hash, bpf_sk_redirect_hash, bpf_lwt_push_encap, bpf_lwt_seg6_store_bytes, bpf_lwt_seg6_adjust_srh, bpf_lwt_seg6_action, bpf_rc_repeat, bpf_rc_keydown, bpf_skb_cgroup_id, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_sk_select_reuseport, bpf_skb_ancestor_cgroup_id, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_msg_push_data, bpf_msg_pop_data, bpf_rc_pointer_rel, bpf_spin_lock, bpf_spin_unlock, bpf_sk_fullsock, bpf_tcp_sock, bpf_skb_ecn_set_ce, bpf_get_listener_sock, bpf_skc_lookup_tcp, bpf_tcp_check_syncookie, bpf_sysctl_get_name, bpf_sysctl_get_current_value, bpf_sysctl_get_new_value, bpf_sysctl_set_new_value, bpf_strtol, bpf_strtoul, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_send_signal, bpf_tcp_gen_syncookie, bpf_skb_output, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_tcp_send_ack, bpf_send_signal_thread, bpf_jiffies64, bpf_read_branch_records, bpf_get_ns_current_pid_tgid, bpf_xdp_output, bpf_get_netns_cookie, bpf_get_current_ancestor_cgroup_id, bpf_sk_assign, bpf_ktime_get_boot_ns, bpf_seq_printf, bpf_seq_write, bpf_sk_cgroup_id, bpf_sk_ancestor_cgroup_id, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_csum_level, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_get_task_stack, bpf_load_hdr_opt, bpf_store_hdr_opt, bpf_reserve_hdr_opt, bpf_inode_storage_get, bpf_inode_storage_delete, bpf_d_path, bpf_copy_from_user, bpf_snprintf_btf, bpf_seq_printf_btf, bpf_skb_cgroup_classid, bpf_redirect_neigh, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_redirect_peer, bpf_task_storage_get, bpf_task_storage_delete, bpf_get_current_task_btf, bpf_bprm_opts_set, bpf_ktime_get_coarse_ns, bpf_ima_inode_hash, bpf_sock_from_file, bpf_check_mtu, bpf_for_each_map_elem, bpf_snprintf, bpf_sys_bpf, bpf_btf_find_by_name_kind, bpf_sys_close
ext	サポート対象外
lsm	サポート対象外

プログラムの種類	利用可能なヘルパー
sk_lookup	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_sk_assign, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf

表7.3 利用可能なマップの種類

マップの種類	Available
ハッシュ	はい
array	はい
prog_array	はい
perf_event_array	はい
percpu_hash	はい
percpu_array	はい
stack_trace	はい
cgroup_array	はい
lru_hash	はい
lru_percpu_hash	はい
lpm_trie	はい
array_of_maps	はい
hash_of_maps	はい
devmap	はい
sockmap	はい

マップの種類	Available
cpumap	はい
xskmap	はい
sockhash	はい
cgroup_storage	はい
reuseport_sockarray	はい
percpu_cgroup_storage	はい
queue	はい
stack	はい
sk_storage	はい
devmap_hash	はい
struct_ops	いいえ
ringbuf	はい
inode_storage	はい
task_storage	いいえ

第8章 バグ修正

ここでは、ユーザーに重大な影響を与えるバグで、Red Hat Enterprise Linux 8.9 で修正されたものについて説明します。

8.1. インストーラーおよびイメージの作成

liveimg の --noverifyssl オプションは、HTTPS を使用してダウンロードされたイメージのサーバーの証明書をチェックしなくなる

以前は、インストーラーは **liveimg** キックスタートコマンドの **--noverifyssl** オプションを無視していました。したがって、HTTPS プロトコルを使用してダウンロードされたイメージに対してサーバーの証明書を検証できない場合、インストールプロセスは失敗しました。今回の更新により、この問題は修正され、**liveimg** キックスタートコマンドの **--noverifyssl** オプションが期待どおりに機能するようになりました。

Bugzilla:1886985

8.2. セキュリティー

NFS ファイルシステムからのブートは、enforcing モードに設定された SELinux で機能するようになる

以前は、NFS をルートファイルシステムとして使用すると、SELinux ラベルがサーバーから転送されず、SELinux が enforcing モードに設定されているときに起動エラーが発生していました。

この修正により、SELinux は、最初の SELinux ポリシーのロード前に作成された NFS マウントにサポートセキュリティーラベルとして正しくフラグを立てるように修正されました。その結果、NFS マウントはサーバーとクライアントの間で SELinux ラベルを転送するようになり、enforcing モードに設定された SELinux でブートを成功させることができます。

Bugzilla:1753646[1]

USB スマートカードリーダーが取り外された場合でも、自動画面ロックが正しく機能するようになりました。

RHEL 8.9 より前では、**opensc** パッケージが USB スマートカードリーダーの取り外しを誤って処理していました。そのため、スマートカードが取り外されたときに画面をロックするように GNOME ディスプレイマネージャー (GDM) を設定しても、システムがロック解除されたままでした。さらに、USB リーダーを再接続してからスマートカードを取り外した後も、画面がロックされませんでした。このリリースでは、USB スマートカードリーダーの取り外しを処理するコードが修正されました。その結果、スマートカードまたは USB スマートカードリーダーが取り外された場合でも、画面が正しくロックされるようになりました。

Bugzilla:2097048

SCAP enable_fips_mode ルールが、64 ビット IBM Z アーキテクチャーで fips=1 のみをチェックするようになりました。

以前は、SCAP セキュリティーガイドルールの **enable_fips_mode** が、**/boot/grub2/grubenv** ファイルの内容をチェックしていました。したがって、64 ビット IBM Z アーキテクチャーでは、FIPS モードに **/boot/grub2/grubenv** ファイルが使用されませんでした。今回の更新により、OVAL ルールの **enable_fips_mode** によって、Linux カーネルの引数 **fips=1** が 64 ビット IBM Z アーキテクチャーの **/boot/loader/entries/.*.conf** ファイルに存在するかどうかテストされるようになりました。

Bugzilla:2129100

SCAP journald ルールが無効な設定に修正されなくなりました。

以前は、SCAP セキュリティーガイドのルール **journald_compress**、**journald_forward_to_syslog**、および **journald_storage** の修復スクリプトにバグが含まれており、**/etc/systemd/journald.conf** 設定ファイル内のそれぞれのオプションに余分な引用符が追加されていました。その結果、**journald** システムサービスは設定オプションの解析に失敗し、それらを無視しました。したがって、設定オプションは効果がなく、OpenSCAP が誤った合格結果を報告していました。この更新により、ルールと修復スクリプトが修正され、余分な引用符が追加されなくなりました。このルールにより、**journald** の有効な設定が作成されるようになりました。

Bugzilla:2169857

セキュリティープロファイルを使用してイメージを設定できるようになりました。

マウントポイントオプションを設定する SCAP セキュリティーガイドのルールが再設計され、Image Builder でオペレーティングシステムのイメージをビルドする際のイメージのハードニングにも、ルールを使用できるようになりました。その結果、特定のセキュリティープロファイルに合わせたパーティション設定でイメージをビルドできるようになりました。

Bugzilla:2130185

AIDE 設定に関連する SSG ルールから厳格な要件を削除しました。

以前は、SCAP セキュリティーガイド (SSG) のルール **aide_build_database** は、**/var/lib/aide/aide.db.new.gz** ファイルと **/var/lib/aide/aide.db.gz** ファイルの両方が存在することを合格の要件としていました。**AIDE** ユーティリティーに **/var/lib/aide/aide.db.new.gz** ファイルが不要になったため、この更新により、**aide_build_database** ルールから対応する要件が削除されました。その結果、ルールの合格要件が **/var/lib/aide/aide.db.gz** ファイルだけになりました。

さらに、SCAP セキュリティーガイドのルール **aide_periodic_cron_checking** の制約が、**/etc/cron.daily** および **/etc/cron.weekly** ファイルのエントリーに対して緩和されました。ルールへの準拠を維持しながら、追加のラッパーを使用して **aide --check** コマンドをスケジュールできるようになりました。

Bugzilla:2175684

pam_faillock に関連する SCAP ルールに不適切な記述が含まれています。

以前は、**pam_faillock** に関連する SCAP セキュリティーガイドのルールに、一部のプロファイル値と整合性がない記述が含まれていました。したがって、記述は正しくありませんでした。今回の更新により、ルールの記述で XCCDF 変数が使用されるようになりました。

この変更は次のルールに影響します。

- **accounts_passwords_pam_faillock_deny**
- **accounts_passwords_pam_faillock_interval**
- **accounts_passwords_pam_faillock_dir**
- **accounts_passwords_pam_faillock_unlock_time**

Bugzilla:2175882

/boot/efi のマウント時に file_permissions_efi_user_cfg SCAP ルールが失敗しなくなりました。

以前は、UEFI ファイルのデフォルトのパーミッションは受け入れられませんでした。したがって、**/boot/efi** パーティションで Virtual File Allocation Table (VFAT) ファイルシステムが使用されてい

る場合は、**chmod** コマンドでパーミッションを変更できませんでした。その結果、**file_permissions_efi_user_cfg** ルールが失敗しました。この更新により、デフォルトのパーミッションが **0600** から **0700** に変更されます。**0700** パーミッションは CIS でも受け入れられるため、評価および修復と CIS プロファイルとの整合性が改善しました。

Bugzilla:2184487

SSG 修復が configure_openssl_cryptopolicy に合わせて調整されました。

以前は、SCAP セキュリティーガイド (SSG) の修復により、**opensslcnf.config** ファイルに **=** 文字が追加されていました。この構文は、**configure_openssl_cryptopolicy** ルールの記述と一致しませんでした。そのため、修復によって **opensslcnf.config** に **.include** の代わりに **.include =** が挿入されると、コンプライアンスチェックが失敗することがありました。このリリースでは、修復スクリプトがルールの記述に合わせて調整され、**configure_openssl_cryptopolicy** を使用する SSG 修復が追加の **=** によって失敗することがなくなりました。

Bugzilla:2192893

postfix_prevent_unrestricted_relay ルールが = 記号の前後の空白を受け入れるようになりました。

以前は、SCAP ルール **xccdf_org.ssgproject.content_rule_postfix_prevent_unrestricted_relay** の OVAL チェックが厳密すぎたため、**=** 記号の前後に空白が含まれる **postconf** 設定割り当てステートメントが考慮されていませんでした。その結果、設定がルールの要件を技術的に満たしていても、このルールは最終レポートで失敗と報告されていました。今回の更新により、**=** 記号の前後に空白があるステートメントをチェックで受け入れるようにルールが変更されました。その結果、最終レポートのルールで、このルールが正しい設定ステートメントに合格しているとマークされるようになりました。

Bugzilla:2170530

SCAP ルールが /var/log および /var/log/audit パーティションが存在するかどうかを正しく評価するようになりました。

以前は、**/var/log** および **/var/log/audit** パーティションに関連する一部の SCAP ルールが、適切なディスクパーティションが存在しない場合でも評価され、修正されていました。これは次のルールに影響を与えました。

- **mount_option_var_log_audit_nodev**
- **mount_option_var_log_audit_noexec**
- **mount_option_var_log_audit_nosuid**
- **mount_option_var_log_nodev**
- **mount_option_var_log_noexec**
- **mount_option_var_log_nosuid**

その結果、ディレクトリー **/var/log** または **/var/log/audit** が個々のパーティションのマウントポイントでない場合でも、これらのルールが評価され、最終レポートで失敗として誤って報告されていました。この更新により、**/var/log** または **/var/log/audit** が個々のパーティションのマウントポイントであるかどうかを判断するための適用性チェックが追加されました。その結果、ディレクトリーが個々のパーティションのマウントポイントではない場合、ルールは設定内で評価されず、最終レポートで **notapplicable** とマークされるようになりました。

Bugzilla:2176008

SCAP ルール accounts_passwords_pam_faillock_interval が新しい STIG ID を対象とするようになりました。

以前は、SCAP セキュリティーガイドのルール **accounts_passwords_pam_faillock_interval** は、RHEL-08-020012 および RHEL-08-020013 を対象としていませんでした。その結果、ルール **accounts_passwords_pam_faillock_interval** は、**/etc/pam.d/password-auth**、**/etc/pam.d/system-auth**、および **/etc/security/faillock.conf** ファイルの **faillock** 設定をチェックしていました。今回の更新により、このルールは STIG ID RHEL-08-020012 および RHEL-08-020013 も対象とするようになりました。

Bugzilla:2209073

Red Hat CVE フィードが更新される

https://access.redhat.com/security/data/oval/ にある Red Hat Common Vulnerabilities and Exposures (CVE) フィードのバージョン 1 は廃止され、https://access.redhat.com/security/data/oval/v2/ にある CVE フィードのバージョン 2 に置き換えられました。

その結果、**scap-security-guide** パッケージによって提供される SCAP ソースデータストリーム内のリンクは、Red Hat CVE フィードの新しいバージョンにリンクするように更新されました。

Bugzilla:2222583

wget ユーティリティーが、制限されたリソースにアクセスするときに TLS ハンドシェイクに失敗しなくなりました。

以前は、TLS でチケットベースのセッション再開が有効になっている場合、制限されたリソースにアクセスするためにサーバーがクライアントに再認証を要求した場合でも、**wget** ユーティリティーは TLS セッションが再開されることを予期していました。この動作により、**wget** は 2 回目の TLS ハンドシェイクに失敗していました。この更新により、**wget** は新しいハンドシェイクを適切に開始するようになり、制限されたリソースへのアクセスが失敗しなくなりました。

Bugzilla:2089817

SELinux が有効なシステムで pam_cap の設定が正しく適用されるようになりました。

以前は、SELinux ポリシーには **pam_cap** モジュールを使用するためのルールが含まれていませんでした。その結果、**/etc/security/capability.conf** 設定ファイルで **pam_cap** によって制御されるログイン機能をユーザーに付与しても、ユーザーが **ssh** またはコンソールを使用してログインした場合、権限の付与が機能しませんでした。この更新により、新しいルールがポリシーに追加されます。その結果、**/etc/security/capability.conf** での機能の付与が機能するようになり、**pam_cap** で設定されたユーザー機能がログイン時に考慮されるようになりました。

Bugzilla:2172541

SELinux が有効なシステムで systemd-fsck-root サービスが正しくラベル付けされるようになりました。

以前は、**/run/fsck** ディレクトリーは **systemd-fsck-root** サービスまたは **fsck** コマンドによって作成されていましたが、SELinux ポリシーにはディレクトリーの適切なラベル付けに関するルールが含まれていませんでした。その結果、**systemd-fsck-root** サービスが正しく動作しませんでした。この更新により、**/run/fsck** の正しいラベルとファイル遷移がポリシーに追加されました。その結果、**systemd-fsck-root** サービスがエラーを報告することなく動作するようになりました。

Bugzilla:2184348[1]

SELinux ポリシーにより D-Bus での双方向通信が許可されるようになりました。

以前は、SELinux ポリシーに、D-Bus メッセージバスシステム上の 2 つのドメイン間で一方向の通信のみを許可するルールが含まれていました。しかし、このような通信は双方向で許可される必要があります。この問題は、Pacemaker 高可用性クラスターリソースマネージャーが **hostnamectl** または **timedatectl** コマンドを実行したときにも発生しました。その結果、Pacemaker がこれらのコマンドを実行すると、SELinux が応答をブロックするため、コマンドが D-Bus 上で応答を受信せずにタイムアウトになりました。SELinux ポリシーのこの更新により、D-Bus での双方向通信が許可されます。その結果、Pacemaker によって実行される、D-Bus での双方向通信を必要とするコマンドが、正常に終了するようになりました。

Bugzilla:2196524

tangd-keygen がデフォルト以外の umask を正しく処理するようになる

以前は、**tangd-keygen** スクリプトは、生成されたキーファイルのファイル権限を変更しませんでした。その結果、他のユーザーへのキーの読み取りを防止するデフォルトのユーザーファイル作成モードマスク (**umask**) が設定されているシステムでは、**tang-show-keys** コマンドはキーを表示する代わりにエラーメッセージ **Internal Error 500** を返していました。今回の更新により、**tangd-keygen** は、生成されたキーファイルのファイルパーミッションを設定するため、スクリプトはデフォルト以外の **umask** を使用するシステムで正しく動作するようになりました。

Bugzilla:2188743

Clevis が SHA-256 サムプリントを処理できるようになりました。

この更新の前は、Clevis クライアントは **thp** 設定オプションで指定された SHA-256 サムプリントを認識しませんでした。その結果、クライアントは SHA-256 サムプリントを使用する Tang サーバーにバインドされず、対応するすべての **clevis encrypt tang** コマンドでエラーが報告されました。今回の更新により、Clevis が SHA-256 を使用してサムプリントを認識し、それらを正しく処理できるようになりました。その結果、Clevis クライアントは、SHA-1 だけでなく SHA-256 サムプリントを使用して Tang サーバーにバインドできるようになりました。

Bugzilla:2209058

Rsyslog は capabilities がなくても起動可能

Rsyslog が通常のユーザーとして実行される場合、またはコンテナー化された環境で実行される場合、**rsyslog** プロセスには capabilities がありません。その結果、Rsyslog は capabilities をドロップできず、起動時に終了しました。今回の更新により、プロセスは、capabilities がない場合に capabilities をドロップしようとしなくなりました。その結果、Rsyslog は capabilities がない場合でも起動できます。

Jira:RHELPLAN-160541[1]

fapolicyd サービスが、信頼されたデータベースから削除されたプログラムを実行しなくなる

以前は、**fapolicyd** サービスは、プログラムが信頼されたデータベースから削除された後でも、プログラムを信頼できるものとして誤って処理していました。その結果、**fapolicyd-cli --update** コマンドを入力しても効果はなく、プログラムは削除された後でも実行される可能性がありました。この更新により、**fapolicyd-cli --update** コマンドによって信頼されたプログラムデータベースが正しく更新され、削除されたプログラムは実行できなくなりました。

Jira:RHEL-630

fapolicyd サービスが正しい所有権を持つ RPM データベースファイルを作成するようになりました。

以前は、**fapolicyd** サービスは **/var/lib/rpm/** ディレクトリーに RPM データベースファイルを作成して所有していました。その結果、他のプログラムがファイルにアクセスできなくなり、可用性制御エラー

が発生していました。この更新により、**fapolicyd** が正しい所有権を持つファイルを作成するようになり、エラーが発生しなくなりました。

Jira:RHEL-829

8.3. ソフトウェア管理

yum needs-restarting -s コマンドで systemd サービスのリストが正しく表示されるようになる

以前は、**needs-restarting** コマンドを **-s** または **--services** オプションとともに使用すると、systemd 以外のプロセスまたは誤動作しているプロセスが検出されたときにエラーが発生していました。今回の更新により、**yum needs-restarting -s** コマンドはそのようなプロセスを無視し、代わりに影響を受ける systemd サービスのリストとともに警告を表示します。

Bugzilla:2122587

dnf-automatic コマンドがトランザクションの終了ステータスを正しく報告するようになる

以前は、**dnf-automatic** コマンドは、トランザクション中の一部のアクションが正常に完了しなかった場合でも、トランザクションの成功終了コードを返しました。これにより、エラータの自動デプロイメントに **dnf-automatic** を使用するマシンでセキュリティーリスクが発生する可能性があります。今回の更新により、この問題は修正され、**dnf-automatic** は、トランザクション中にパッケージに関するすべての問題を報告するようになりました。

Bugzilla:2170093

YUM は proxy=_none_ を正しく処理するようになりました

YUM **proxy=_none_** 設定オプションを使用すると、プロキシー設定の変更を禁止できます。以前は、メイン設定ファイルで **proxy=_none_** を設定すると、YUM によってエラーが検出されました。この更新によりバグが修正され、YUM が **proxy=_none_** を正しく処理できるようになりました。

注記

RHEL 8 の YUM **proxy=_none_** 設定は、RHEL 7 の YUM 設定と互換性があります。

Bugzilla:2155713

dbus が所有するファイルが zlib によって更新された場合に、needs-restarting プラグインがシステムの再起動を正しく要求するようになりました。

以前は、YUM **needs-restarting** プラグインを実行すると、**dbus** パッケージが所有するファイルが、依存する **zlib** パッケージによって更新されたときに、システムの再起動を求めるプロンプトが表示されませんでした。今回の更新により、この問題が修正され、**zlib** の更新時に **dbus** を再起動する必要があるという内容のメッセージを **needs-restarting** プラグインが表示するようになりました。

Bugzilla:2092033

8.4. シェルおよびコマンドラインツール

which コマンドが長いパスでも失敗しなくなる

以前は、パスが 256 文字を超えるディレクトリーで **which** コマンドを実行すると、**Can't get current working directory** というエラーメッセージが表示されてコマンドが失敗していました。この修正により、**which** コマンドはパスの長さの制限として **PATH_MAX** 値を使用するようになりました。その結果、コマンドは失敗しなくなりました。

Bugzilla:2140566

ReaR は OUTPUT=USB で UEFI セキュアブートをサポートするようになる

以前は、ブータブルディスクドライブにレスキューイメージを保存する **OUTPUT=USB** ReaR 出力メソッドは、**SECURE_BOOT_BOOTLOADER** 設定を尊重しませんでした。その結果、UEFI セキュアブートが有効になっているシステムでは、ブートローダーが署名されていないため、レスキューイメージを含むディスクは起動しませんでした。

この修正により、**OUTPUT=USB** ReaR 出力メソッドは、レスキューディスクの作成時に **SECURE_BOOT_BOOTLOADER** 設定で指定したブートローダーを使用するようになりました。署名付き UEFI shim ブートローダーを使用するには、**/etc/rear/local.conf** ファイルで次の設定を変更します。

```
SECURE_BOOT_BOOTLOADER=/boot/efi/EFI/redhat/shimx64.efi
```

この結果、UEFI セキュアブートが有効になっている場合、レスキューディスクは起動可能になります。セキュアブートが有効になっていない場合でも、UEFI を備えたすべてのシステムで変数をこの値に安全に設定できます。一貫性を保つためにも推奨されます。UEFI ブート手順と shim ブートローダーの詳細は、UEFI: what happens when booting the system 参照してください。

Bugzilla:2233526

SEL 要求がタイムアウトしたときに、ipmievd が SEL 応答を正しく認識するようになりました。

ipmievd サービスは、**/dev/ipmi0** デバイス経由でシステムイベントログ (SEL) 要求を送信します。以前は、返された IPMI メッセージの ID チェックが欠落していたため、要求がタイムアウトすると、次の応答が正しく処理されませんでした。たとえば、ベースボード管理コントローラー (BMC) がリセットされた場合、**ipmievd** サービスからの SEL 要求が、SEL 応答がないためにタイムアウトになりました。そのため、対応しない SEL 応答により、**ipmievd** が正しく動作しませんでした。その結果、正しいハードウェア状態が取得されず、大量の誤ったハードウェア情報が **/var/log/messages** に出力されました。この修正により、**ipmitool** と **ipmievd** が、返された IPMI メッセージの ID を要求の ID と照合してチェックし、対応しない SEL 要求をスキップするようになりました。**ipmevd** が誤ったハードウェア情報をログに記録しなくなりました。

Bugzilla:2224567[1]

8.5. ネットワーク

Intel Corporation I350 Gigabit Fiber Network Connection は、カーネル更新後にリンクを提供するようになる

以前は、External Thermal Sensor (ETS) のない Small Formfactor Pluggable (SFP) トランシーバーモジュールを使用したハードウェア設定により、**igb** ドライバーが ETS を読み取るために Inter-Integrated Circuit (I2C) を誤って初期化していました。その結果、接続はリンクを取得できませんでした。このバグ修正により、**igb** ドライバーは、ETS を備えた SFP が使用可能な場合にのみ I2C を初期化します。その結果、接続はリンクを取得します。

Bugzilla:2130727[1]

8.6. ブートローダー

grubby は引数を新しいカーネルに正しく渡すようになりました。

grubby ツールを使用して新しいカーネルを追加し、引数を指定しないか、引数を空白のままにすると、**grubby** は新しいカーネルに引数を渡さず、**root** は設定されません。**--args** および **--copy-default** オプションを使用すると、新しい引数がデフォルトの引数に追加されます。

Bugzilla:1900829

8.7. ファイルシステムおよびストレージ

multipathd が永続予約登録キーをすべてのパスに追加する

以前は、**multipathd** デーモンが起動して、既存のマルチパスデバイスの 1 つのパス上の永続予約登録キーを認識したとき、そのデバイスのすべてのパスに登録キーがあるわけではありませんでした。その結果、**multipathd** が停止している間に永続予約を持つマルチパスデバイスに新しいパスが現れた場合、それらのパスには永続予約はセットアップされませんでした。これにより、予約キーによって禁止されているはずのパス上での IO 処理が可能になりました。

この修正により、**multipathd** がデバイスパス上で永続予約登録キーを見つけた場合、そのキーをすべてのアクティブなパスに追加します。その結果、**multipathd** が実行されていないときにパスデバイスが最初に表示された場合でも、multipath デバイスではすべてのパス上で永続予約が正しくセットアップされるようになりました。

Bugzilla:2164871

OS のインストール中に LUN が表示されるようになる

以前は、特に iSCSI iBFT (Boot Firmware Table) に保存されている CHAP (Challenge-Handshake Authentication Protocol) 認証による iSCSI ハードウェアオフロードが関係する場合、システムはファームウェアソースからの認証情報を使用していませんでした。その結果、インストール中に iSCSI ログインが失敗しました。

udisks2-2.9.4-9.el9 ファームウェア認証の修正により、この問題は解決され、インストールおよび初回起動時に LUN が表示されるようになりました。

Bugzilla:2213193[1]

8.8. 高可用性およびクラスター

保留中のアクションがすべて完了するまで、Pacemaker Designated Controller の選出が確定しなくなりました。

クラスターが新しい Designated Controller (DC) を選出すると、すべてのノードが現在の履歴を新しい DC に送信し、CIB に保存します。その結果、新しい DC が選出されたときにアクションがすでに進行中で、ノードが現在の履歴を新しい DC に送信した後にアクションが終了した場合、アクションの結果が失われる可能性がありました。この修正により、保留中のアクションがすべて完了し、アクションの結果が失われることがなくなるまで、DC の選出が確定しなくなりました。

Bugzilla:2010084

fence_scsi エージェントが共有 lvmlockd デバイスを自動検出できるようになる

以前は、**fence_scsi** エージェントは共有 **lvmlockd** デバイスを自動検出しませんでした。今回の更新により、**fence_scsi** は、**devices** 属性が設定されていない場合に、**lvmlockd** デバイスを自動検出できるようになりました。

Bugzilla:2187329

リソースのスティッキネスがコロケーションスコアと適切に比較されるようになりました。

チェーンリソースコロケーションは、割り当て中のリソースと同じ場所にあるリソースです。以前は、元のコロケーションに有限の負のスコアがあり、チェーンコロケーションが必須の場合、resource-stickiness が **INFINITY** に設定されている場合でも、割り当て中の元のリソースがそのノードから禁止される可能性がありました。この修正により、チェーンコロケーションが比例的に考慮されるようになり、スティッキネスがコロケーションスコアと適切に比較されるようになりました。

Bugzilla:1632951[1]

crm_resource コマンドで、アクティブなレプリカが 1 つだけあるバンドルを禁止または移動できるようになりました。

以前は、**crm_resource** コマンドが、単一のレプリカを持つバンドルがアクティブな場所をチェックするときに、アクティブなコンテナーを持つノードと、コンテナー自体に対して作成されたゲストノードの両方をカウントしていました。その結果、**crm_resource** コマンドは、単一のアクティブなレプリカを持つバンドルの禁止や移動を行いませんでした。この修正により、**crm_resource** コマンドは、アクティブなレプリカの数を決定するときに、バンドルのコンテナーがアクティブなノードのみをカウントするようになりました。

Bugzilla:1578820

mysql リソースエージェントがプロモート可能なクローンリソースで正しく動作するようになる

以前は、プロモートされた値とプロモートされていない値の間でプロモーションスコアが変化するため、**mysql** リソースエージェントは Master ロールで動作しているクローンリソースをノード間で移動していました。この修正により、昇格されたノードは昇格されたままになります。

Bugzilla:2039692

プロモートされていないクローンインスタンスが不必要に再起動されなくなりました。

以前は、プロモート可能なクローンインスタンスは、プロモートされたインスタンスが最初となる番号順に割り当てられていました。その結果、プロモートされたクローンインスタンスを起動する必要がある場合、インスタンス番号が変更されたため、プロモートされていないインスタンスが予期せず再起動する場合がありました。この修正により、ノードにインスタンス番号を割り当てるときにロールが考慮されるようになり、その結果、不要な再起動が発生しなくなります。

Bugzilla:1931023

2 番目のフェンシングデバイスとして設定されたフェンス watchdog は、最初のデバイスがタイムアウトになったときにノードをフェンスするようになる

以前は、watchdog フェンシングデバイスがフェンシングトポロジーの 2 番目のデバイスとして設定されている場合、フェンシング操作のタイムアウトを計算するときに watchdog タイムアウトは考慮されませんでした。その結果、最初のデバイスがタイムアウトすると、watchdog がノードをフェンスしても、フェンシング操作はタイムアウトになります。この修正により、watchdog タイムアウトがフェンシング操作のタイムアウトに含まれ、最初のデバイスがタイムアウトになった場合にフェンシング操作は成功します。

Bugzilla:2168633

リストがノードごとにグループ化されている場合、ルールを含む場所の制約が表示されなくなる

ルールを含むロケーション制約にはノードを割り当てることができません。以前は、ノードごとにリストをグループ化すると、ルールを含む場所の制約が空のノードの下に表示されていました。この修正に

より、ルールのある場所の制約は表示されなくなり、ルールのある制約が表示されないことを示す警告が表示されます。

Bugzilla:2166294

マルチパス SCSI デバイスを更新する pcs コマンドが正しく動作するようになる

Pacemaker CIB ファイルの変更により、**pcs stonith update-scsi-devices** コマンドが設計どおりに動作しなくなり、一部のクラスターリソースが望ましくない再起動を引き起こしました。この修正により、このコマンドは正しく機能し、同じノード上で実行されている他のクラスターリソースを再起動することなく SCSI デバイスを更新できるようになりました。

Bugzilla:2179010

pscd Web UI が開いているときに pcsd-ruby デーモンのメモリーフットプリントが削減されるようになる

以前は、**pcsd** Web UI が開いていると、 **pcsd-ruby** デーモンのメモリー使用量が数時間にわたって着実に増加していました。この修正により、**pcsd-ruby** デーモンで実行される Web サーバーが定期的にグレースフルリスタートを実行するようになりました。これにより、割り当てられたメモリーが解放され、メモリーフットプリントが削減されます。

Bugzilla:2189958[1]

azure-events-az リソースエージェントが Pacemaker 2.1 以降でエラーを生成しなくなる

azure-events-az リソースエージェントは **crm_simulate -Ls** コマンドを実行し、出力を解析します。Pacemaker 2.1 以降では、**crm_simulate** コマンドの出力に **Transition Summary:** というテキストが含まれなくなり、エラーが発生しました。この修正により、このテキストが欠落している場合でもエージェントはエラーを生成しなくなりました。

Bugzilla:2181019

8.9. コンパイラーおよび開発ツール

guru モードを使用した systemtap スクリプトがより速くコンパイルされるようになりました。

systemtap の guru モードの liveness 分析では、 **dyninst** ライブラリーを使用してバイナリーを解析します。新しいカーネルは、**CONFIG_RETPOLINE=y** を使用して軽減コードを有効にし、従来の RET 命令をサンクへのジャンプで置き換えます。その結果、サンクへのジャンプによって導入された制御フローグラフの追加のエッジを liveness 分析ですべて検査する必要があるため、バイナリー解析にはるかに長い時間がかかりました。

今回の更新により、カーネルコードがサンクを使用している場合、**systemtap** が liveness 分析を無効にします。その結果、guru モードを使用する **systemtap** スクリプトのコンパイルがより速くなります。

Bugzilla:2126805

eu-addr2line -C が他の引数を正しく認識するようになる

以前は、**elfutils** の **eu-addr2line** コマンドで **-C** 引数を使用すると、次の 1 文字の引数が消えていました。その結果、**eu-addr2line -Ci** コマンドは **eu-addr2line -C** と同じように動作し、**eu-addr2line -iC** は期待どおりに動作しました。このバグは修正され、**eu-addr2line -Ci** は 両方の引数を認識するようになりました。

Bugzilla:2236183

eu-addr2line -i は、GCC リンクタイム最適化でコンパイルされたコードを正しく処理するようになる

以前は、**elfutils** に含まれる **libdw** ライブラリーの **dwarf_getscopes** 関数は、GCC リンクタイム最適化でコンパイルされた関数の抽象オリジン定義を見つけることができませんでした。したがって、**eu-addr2line** コマンドで **-i** 引数を使用すると、**eu-addr2line** は **gcc -flto** でコンパイルされたコードのインライン関数を表示できませんでした。今回の更新により、**libdw dwarf_getscopes** 関数はインライン化スコープの正しいコンパイル単位を検索し、**eu-addr2line -i** は 期待どおりに動作するようになりました。

Bugzilla:2162495

8.10. IDENTITY MANAGEMENT

SSSD が GPO ベースのアクセス制御を評価するときに sAMAccountName を使用するようになる

以前は、AD クライアントで **ldap_user_name** が **sAMAccountName** 以外の値に設定されている場合、GPO ベースのアクセス制御が失敗しました。今回の更新により、SSSD が GPO ベースのアクセス制御を評価するときに常に **sAMAccountName** を使用するようになりました。**ldap_user_name** が AD クライアントの **sAMAccountName** とは異なる値に設定されている場合でも、GPO ベースのアクセス制御が正しく機能するようになりました。

Jira:SSSD-6107

SSSD は、ユーザーを取得するときに user_attributes オプションで重複した属性を処理するようになる

以前は、**sssd.conf** が **user_attributes** オプションに重複した属性を含んでいた場合、SSSD はこれらの重複を正しく処理しませんでした。その結果、それらの属性を持つユーザーを取得できませんでした。この更新により、SSSD は重複を正しく処理できるようになりました。その結果、重複した属性を持つユーザーを取得できるようになりました。

Jira:SSSD-6177

セキュリティーパラメーターの変更が正しく機能するようになる

以前は、**dsconf instance_name security set** コマンドを使用してセキュリティーパラメーターを変更すると、次のエラーが発生して操作が失敗していました。

```
Name 'log' is not defined
```

この更新により、セキュリティーパラメーターの変更が期待どおりに機能するようになりました。

Bugzilla:2166284

Directory Server が、開いている記述子の最大数に基づいて dtablesize を計算するようになりました。

以前は、管理者は **nsslapd-conntablesize** 設定パラメーターを使用して、接続テーブルのサイズを手動で設定できました。そのため、接続テーブルのサイズ設定が小さすぎると、サーバーがサポートできる接続数に影響が及んでいました。今回の更新により、Directory Server が接続テーブルのサイズを動的に計算するようになり、接続テーブルのサイズが小さすぎる問題を効果的に解決できるようになりました。さらに、接続テーブルのサイズを手動で変更する必要がなくなりました。

Bugzilla:2210491

dsctl healthcheck コマンドがデフォルトでパスワード保存スキーム PBKDF2-SHA512 を使用するようになりました。

以前は、**dsctl healthcheck** コマンドはデフォルトで **SSHA512** パスワード保存スキームを使用していました。その結果、新しいパスワード保存スキーム **PBKDF2-SHA512** が検出されなかったため、このコマンドは警告を報告していました。今回の更新により、**dsctl healthcheck** コマンドがデフォルトで **PBKDF2-SHA512** パスワード保存スキームを使用するようになり、警告が発生しなくなりました。

Bugzilla:2220890

通常のユーザーによるページ検索はパフォーマンスに影響を与えなくなる

以前は、Directory Server に検索負荷がかかっている場合、ロックがネットワークイベントをポーリングするスレッドと競合するため、通常のユーザーからのページ検索がサーバーのパフォーマンスに影響を与える可能性がありました。さらに、ページ検索の送信中にネットワークの問題が発生した場合、**nsslapd-iotimeout** パラメーターの期限が切れるまでサーバー全体が応答しなくなっていました。今回の更新では、ネットワークイベントとの競合を避けるために、ロックがいくつかの部分に分割されました。その結果、一般ユーザーからのページ検索中のパフォーマンスへの影響はありません。

Bugzilla:2224505

Directory Server で暗号を期待どおりに有効または無効にできるようになりました。

以前は、Web コンソールを使用してデフォルトの暗号に加えて特定の暗号を有効または無効にしようとすると、サーバーが特定の暗号のみを有効または無効にし、次のようなエラーをログに記録していました。

```
Security Initialization - SSL alert: Failed to set SSL cipher preference information: invalid ciphers
<default,+cipher_name>: format is +cipher1,-cipher2... (Netscape Portable Runtime error 0 - no error)
```

現在、ネットワークセキュリティーサービス (NSS) は、デフォルトの暗号と特定の暗号を同時に処理することをサポートしていません。そのため、Directory Server は特定の暗号またはデフォルトの暗号を有効または無効にすることができます。今回の更新により、デフォルトの暗号を設定すると、Web コンソールで **Allow Specific Ciphers** フィールドと **Deny Specific Ciphers** フィールドがクリアされることを示すメッセージが表示されるようになりました。

Bugzilla:1817505

IdM admin ユーザーの削除が許可されなくなる

以前は、**admin** グループのメンバーであれば、Identity Management (IdM) の **admin** ユーザーを削除できました。**admin** ユーザーが存在しないと、IdM と Active Directory (AD) の間の信頼が正しく機能しません。この更新により、**admin** ユーザーを削除できなくなりました。結果として、IdM-AD 信頼は正しく機能します。

Bugzilla:1821181

IdM クライアントは、信頼できる AD ユーザーの名前に大文字と小文字が混在している場合でも、当該 AD ユーザーの情報を適切に取得する

以前は、ユーザーの検索または認証を試行した際に、その信頼できる Active Directory (AD) ユーザーの名前に大文字と小文字が混在しており、かつ IdM でオーバーライドが設定されていた場合、エラーが返され、ユーザーは IdM リソースにアクセスできませんでした。

RHBA-2023:4525 のリリースにより、大文字と小文字を区別する比較は、大文字と小文字を区別しない比較に置き換えられました。その結果、IdM クライアントは、ユーザー名に大文字と小文字が混在しており、IdM でオーバーライドが設定されている場合でも、AD の信頼済みドメインのユーザーを検索できるようになりました。

Jira:SSSD-6096

8.11. グラフィックインフラストラクチャー

ASPEED 2600 を搭載したサーバーでインストーラーがフリーズしなくなりました。

以前は、ASPEED 2600 On System Management チップセットを搭載したサーバーでグラフィカル RHEL 8.8 インストーラーを起動すると、ブラックスクリーンが表示されて応答しなくなりました。そのため、サーバーに RHEL 8.8 をインストールできませんでした。

このリリースでは、この問題は修正されています。そのため、ASPEED 2600 搭載サーバーでインストールが期待どおりに進むようになりました。

Bugzilla:2189645[1]

8.12. WEB コンソール

Web コンソールの NBDE バインディング手順が、ルートファイルシステムを持つボリュームグループで機能するようになる

RHEL 8.8 では、ユーザーがルートファイルシステムに Tang キーを追加したかどうかを判断するコードのバグが原因で、LUKS コンテナー上にファイルシステムがまったく存在しない場合、Web コンソールのバインドプロセスがクラッシュしました。**Verify key** ダイアログの **Trust key** ボタンをクリックした後、Web コンソールにエラーメッセージ **TypeError: Qe(...) is undefined** が表示されたため、説明されているシナリオのコマンドラインインターフェイスで必要な手順をすべて実行する必要がありました。

この更新により、Web コンソールはルートファイルシステムへの Tang キーの追加を正しく処理できるようになりました。その結果、Web コンソールは、さまざまなシナリオで Network-Bound Disk Encryption (NBDE) を使用した LUKS 暗号化ボリュームの自動ロック解除に必要なバインド手順をすべて完了します。

Bugzilla:2212350

VNC コンソールがほとんどの解像度で機能するようになる

以前は、特定のディスプレイ解像度で Virtual Network Computing (VNC) コンソールを使用すると、マウスオフセットの問題が発生したり、インターフェイスの一部しか表示されなかったりしました。そのため、VNC コンソールを使用することはできませんでした。

今回の更新で問題が修正され、3840x2160 などの超高解像度を除き、VNC コンソールが最大解像度で正しく機能するようになりました。

カーソルの録画した位置と表示位置の間には、小さいオフセットが引き続き存在する可能性があることに注意してください。ただし、これは VNC コンソールのユーザービリティーに大きな影響を与えることはありません。

Bugzilla:2030836

8.13. RED HAT ENTERPRISE LINUX システムロール

storage ロールが、アンマウントせずにマウントされたファイルシステムのサイズを変更できるようになる

以前は、ファイルシステムがオンラインサイズ変更をサポートしていても、**storage** ロールはマウントされたデバイスのサイズを変更できませんでした。その結果、**storage** ロールはサイズ変更の前にすべ

てのファイルシステムをアンマウントしましたが、実行中のシステムの / ディレクトリーのサイズ変更中など、使用中のファイルシステムでは失敗しました。

この更新により、**storage** ロールは、XFS や Ext4 などのオンラインサイズ変更をサポートする、マウントされたファイルシステムのサイズ変更をサポートするようになりました。その結果、マウントされたファイルシステムをアンマウントせずにサイズ変更できるようになりました。

Bugzilla:2168738

certificate RHEL システムロールが、新しい証明書要求を実行するかどうかを決定するときに証明書のキーサイズをチェックするようになる

以前は、**certificate** RHEL システムロールは、新しい証明書を要求するかどうかを評価するときに、証明書のキーサイズをチェックしませんでした。その結果、同ロールは、新しい証明書要求を発行すべき場合に、発行しないことがありました。この更新により、**certificate** は **key_size** パラメーターをチェックして、新しい証明書要求を実行する必要があるかどうかを判断するようになりました。

Bugzilla:2186057

rhc ロールを使用して作成された Insights タグが正しく適用されるようになる

以前は、**rhc** ロールを使用して Insights タグを作成した場合、タグは正しいファイルに保存されませんでした。そのため、タグは Insights に送信されず、その結果、タグは Insights インベントリー内のシステムに適用されませんでした。

この修正により、タグが正しく保存され、Insights インベントリーに存在するシステムに適用されるようになりました。

Bugzilla:2209441

RHEL 7 の firewall RHEL システムロールが存在しない Python パッケージのインストールを試行しなくなる

以前は、RHEL 7 の **firewall** ロールが別のロールから呼び出され、そのロールが **python3** を使用していた場合、**firewall** ロールはそのバージョンの Python の **python3-firewall** ライブラリーをインストールしようとしていました。ただし、そのライブラリーは RHEL 7 では利用できません。そのため、**python3-firewall** ライブラリーが見つからず、次のエラーメッセージが表示されていました。

```
No package matching 'python3-firewall' found available, installed or updated
```

今回の更新で、**firewall** ロールは、**python-firewall** または **python3-firewall** ライブラリーのインストールを試行しなくなりました。その結果、マネージドノードに **python3** がインストールされている場合、RHEL 7 で **firewall** ロールは失敗しません。

Bugzilla:2216521

作成前にメンバーディスクからデータを削除できなかった問題が解消される

以前は、RAID ボリュームを作成するときに、システムは RAID ボリュームを形成する前にメンバーディスクから既存のデータを効果的に削除しませんでした。この更新により、RAID ボリュームは必要に応じてメンバーディスクから既存のデータを削除します。

Bugzilla:2224094

podman_registries_conf 変数で unqualified-search-registries フィールドが正しく設定されるようになる

以前は、**podman_registries_conf** 変数を設定した後、**podman** RHEL システムロールが失敗していま

した。その結果、**unqualified-search-registries = ["registry.access.redhat.com"]** 設定は、**/etc/containers/registries.conf.d/50-systemroles.conf** ファイルに生成されませんでした。今回の更新で、この問題が修正されています。

Bugzilla:2226077

raid_chunk_size パラメーターがエラーメッセージを返さなくなる

以前は、**raid_chunk_size** 属性は、RAID プールおよびボリュームに対して許可されていませんでした。この更新により、制限を受けることなく RAID プールおよびボリュームの **raid_chunk_size** 属性を設定できるようになりました。

Bugzilla:2193057

存在しないサービスを使用して firewall RHEL システムロールをチェックモードで実行しても失敗しなくなる

以前は、存在しないサービスを使用してチェックモードで **firewall** ロールを実行すると失敗していました。この修正により、チェックモードの Ansible ベストプラクティスへの準拠性が向上しました。その結果、存在しないサービスが有効または無効でも、チェックモードのロールは失敗しなくなりました。代わりに、サービスが以前の Playbook で定義されていることを確認する警告が表示されます。

Bugzilla:2222433

kdump ロールが authorized_keys をべき等性を持たせて追加する

以前は、**authorized_key** を追加するタスクは毎回余分な改行文字を追加していました。そのため、ロールはべき等性を持ちませんでした。この修正により、新しい **authorized_key** の追加は正しく機能し、単一のキー値のみをべき等性を持たせて追加します。

Bugzilla:2232391

authorized_keys がない場合も、kdump システムロールが失敗しなくなりました。

以前は、**kdump_ssh_user** 変数で定義されたユーザーが **home** ディレクトリー内の **.ssh** ディレクトリーまたは空の **.ssh/authorized_keys** ファイルにアクセスできない場合、**kdump** システムロールは **SSH** 認可キーを追加できませんでした。この修正により、**kdump** システムロールは認可されたキーを **SSH** 設定に正しく追加するようになりました。その結果、キーベースの認証は、説明したシナリオで確実に機能します。

Bugzilla:2232392

firewall RHEL システムロールが、チェックモードで previous: replaced を使用するときに変更を正しく報告するようになる

以前は、**previous: replaced** ロールは、チェックモードで **previous: replaced** パラメーターを使用するときに、ファイルの変更についてチェックしていませんでした。その結果、ロールでは未定義の変数に関するエラーが発生しました。この修正により、**previous: replaced** パラメーターによるファイルの変更を評価する新しいチェック変数がチェックモードに追加されました。**firewalld.conf** ファイルのチェックでは、**rpm** データベースを評価して、ファイルがパッケージに同梱されているバージョンから変更されているか判断します。その結果、**firewall** ロールは、**previous: replaced** パラメーターを使用する場合、変更を正しく報告するようになりました。

Jira:RHEL-899[1]

システムロールに対して kdump を有効にするには、RHEL 9 以降のバージョンで failure_action 設定パラメーターを使用する必要があります。

以前は、**kdump** 設定中に **default** オプションを使用すると成功せず、以下の警告がログに出力されていました。

```
kdump: warning: option 'default' was renamed 'failure_action' and will be removed in the future.
please update /etc/kdump.conf to use option 'failure_action' instead.
```

その結果、**default** オプションが使用されていた場合、ロールは **kdump** を正常に有効にしませんでした。今回の更新で問題が修正され、**failure_action** パラメーターを使用して、複数のシステムにカーネルダンプパラメーターを設定できるようになりました。これにより、上述のシナリオで **kdump** の有効化が正常に機能します。

Jira:RHEL-907[1]

firewall RHEL システムロールが、Network Manager インターフェイスにゾーンを割り当てるときに変更を正しく報告するようになる

以前は、Network Manager インターフェイス割り当ては、変更が存在しない場合でも変更を報告していました。この修正により、**library/firewall_lib.py** ファイル内の **try_set_zone_of_interface** モジュールは、インターフェイスのゾーンが変更されたかどうかを示す 2 番目の値を返します。その結果、Network Manager によって処理されるインターフェイスにゾーンを割り当てるときに、モジュールは変更を正しく報告するようになりました。

Jira:RHEL-918[1]

kdump ロールにより、kdump_ssh_server 認証の .ssh/authorized_keys が正常に更新されます。

以前は、**kdump** ロールが **.ssh** ディレクトリーにアクセスして、**kdump_ssh_server** にログインするためのユーザーを安全に認証できませんでした。その結果、**kdump** ロールは、**kdump_ssh_server** が失敗したことを確認するための **.ssh/authorized_keys** ファイルと SSH メカニズムを更新しませんでした。今回の更新でこの問題が修正されています。これにより、**kdump_ssh_server** の **kdump_ssh_user** 認証が確実に機能します。

Jira:RHEL-1398[1]

firewall システムロールの previous: replaced パラメーターが、以前の設定を削除せずにオーバーライドするようになる

以前は、変数リストに **previous: replaced** パラメーターを追加すると、**firewall** システムロールは既存のユーザー定義設定をすべて削除し、**firewalld** をデフォルト設定にリセットしていました。この修正では、EL7 リリースで導入された **firewalld** のフォールバック設定を使用して、以前の設定を保持します。その結果、変数リストで **previous: replaced** パラメーターを使用すると、**firewall.conf** 設定ファイルはリセット時に削除されませんが、ファイルとファイル内のコメントが保持されます。

Jira:RHEL-1496[1]

kdump ロールは、複数のキーを authorized_keys にべき等性を持たせて追加する

以前は、**authorized_keys** ファイルに複数の SSH キーを同時に追加すると、あるホストのキー値が別のホストに置き換えられていました。この更新では、**lineinfile** モジュールを使用して **authorized_keys** ファイルを管理することで問題が修正されます。**lineinfile** はタスクを順番に繰り返し処理し、既存のキーをチェックし、1 つのホストで一度に新しいキーを 1 つのアトミック操作で書き込みます。その結果、複数のホストに SSH キーを追加すると正しく機能し、別のホストのキーの値を置き換えません。

注記: **serial: 1** play serial キーワードを play レベルで使用して、1 度に実行されているホストの数を制御します。

Jira:RHEL-1500[1]

8.14. 仮想化

仮想マシンへの Watchdog カードのホットプラグが失敗しなくなる

以前は、使用可能な PCI スロットがない場合、実行中の仮想マシン (VM) に Watchdog カードを追加すると、以下のエラーが発生し、失敗していました。

> Failed to configure watchdog
> ERROR Error attempting device hotplug: internal error: No more available PCI slots

今回の更新で問題が修正され、実行中の仮想マシンに Watchdog カードを追加すると、想定どおりに機能するようになりました。

Bugzilla:2173584

第9章 テクノロジープレビュー

ここでは、Red Hat Enterprise Linux 8.9 で利用可能なテクノロジープレビューのリストを提示します。

テクノロジープレビューに対する Red Hat のサポート範囲の詳細は、テクノロジープレビューのサポート範囲 を参照してください。

9.1. インフラストラクチャーサービス

TuneD 用のソケット API がテクノロジープレビューとして利用可能になる

UNIX ドメインソケットを通じて TuneD を制御するためのソケット API がテクノロジープレビューとして利用可能になりました。ソケット API は D-Bus API と 1 対 1 でマッピングされ、D-Bus が利用できない場合に代替通信方法を提供します。ソケット API を使用すると、TuneD デーモンを制御してパフォーマンスを最適化したり、さまざまなチューニングパラメーターの値を変更したりできます。ソケット API はデフォルトでは無効になっていますが、**tuned-main.conf** ファイルで有効にできます。

Bugzilla:2113900

9.2. ネットワーク

AF_XDP がテクノロジープレビューとして利用可能に

AF_XDP (**Address Family eXpress Data Path**) ソケットは、高性能パケット処理用に設計されています。さらに処理するために、**XDP** を取り入れ、プログラムにより選択されたパケットの効率的なリダイレクトをユーザー空間アプリケーションに付与します。

Bugzilla:1633143[1]

テクノロジープレビューとして利用できる XDP 機能

Red Hat は、以下の eXpress Data Path (XDP) 機能をサポート対象外のテクノロジープレビューとして提供します。

- AMD および Intel 64 ビット以外のアーキテクチャーで XDP プログラムを読み込む。**libxdp** ライブラリーは、AMD および Intel 64 ビット以外のアーキテクチャーでは使用できません。
- XDP ハードウェアオフロード。

Bugzilla:1889737

TC のマルチプロトコルラベルスイッチがテクノロジープレビューとして利用可能に

Multi-protocol Label Switching (MPLS) は、エンタープライズネットワーク全体でトラフィックフローをルーティングするカーネル内データ転送メカニズムです。MPLS ネットワークでは、パケットを受信するルーターは、パケットに割り当てられたラベルに基づいて、パケットの追加のルートを決定します。ラベルを使用すると、MPLS ネットワークは特定の特性を持つパケットを処理する機能があります。たとえば、特定ポートから受信したパケットの管理や、特定のタイプのトラフィックを一貫した方法で伝送する **tc filters** を追加できます。

パケットがエンタープライズネットワークに入ると、MPLS ルーターは、パケット上で複数の操作を実行します。ラベルの追加には **push**、**swap** (ラベルの更新)、ラベルの削除の **pop** などが含まれます。MPLS では、RHEL の 1 つまたは複数のラベルに基づいて、アクションをローカルに定義できます。ルーターを設定し、トラフィック制御 (**tc**) フィルターを設定して、**label**、**traffic class**、**bottom of stack**、**time to live** などの MPLS ラベルスタックエントリー (**lse**) 要素に基づいて、パケットに対して適切なアクションを実行するように設定することができます。

たとえば、次のコマンドは、フィルターを **enp0s1** ネットワークインターフェイスに追加して、最初のラベル **12323** と 2 番目のラベル **45832** を持つ着信パケットと一致させます。一致するパケットでは、以下のアクションが実行されます。

- 最初の MPLS TTL はデクリメントされます (TTL が 0 に達するとパケットがドロップされます)。
- 最初の MPLS ラベルが **549386** に変更
- 作成されるパケットは **enp0s2** 経由で送信されます。宛先 MAC アドレス **00:00:5E:00:53:01**、およびソース MAC アドレス **00:00:5E:00:53:02**。

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

Bugzilla:1814836[1]、Bugzilla:1856415

act_mpls モジュールがテクノロジープレビューとして利用可能になりました。

act_mpls モジュールが、テクノロジープレビューとして **kernel-modules-extra** rpm で利用可能になりました。モジュールを使用すると、トラフィック制御 (TC) フィルターを使用した Multiprotocol Label Switching (MPLS) アクション (TC フィルターを使用した MPLS ラベルスタックエントリーの push や pop など) の適用が可能になります。また、このモジュールでは、Label、Traffic Class、Botem of Stack、および Time to Live フィールドを独立して設定できます。

Bugzilla:1839311[1]

systemd-resolved サービスがテクノロジープレビューとして利用できるようになりました。

systemd-resolved サービスは、ローカルアプリケーションに名前解決を提供します。このサービスは、DNS スタブリゾルバー、LLMNR (Link-Local Multicast Name Resolution)、およびマルチキャスト DNS リゾルバーとレスポンダーのキャッシュと検証を実装します。

systemd パッケージが **systemd-resolved** を提供している場合でも、このサービスはサポートされていないテクノロジープレビューであることに注意してください。

Bugzilla:1906489

9.3. カーネル

テクノロジープレビューとして利用できる Soft-RoCE

Remote Direct Memory Access (RDMA) over Converged Ethernet (RoCE) は、RDMA over Ethernet を実装するネットワークプロトコルです。Soft-RoCE は、RoCE v1 および RoCE v2 の 2 つのプロトコルバージョンを維持する RoCE のソフトウェア実装です。Soft-RoCE ドライバーの **rdma_rxe** は、RHEL 8 ではサポートされていないテクノロジープレビューとして利用できます。

Bugzilla:1605216[1]

eBPF がテクノロジープレビューとして利用可能になりました。

eBPF (extended Berkeley Packet Filter)は、限られた一連の関数にアクセスできる制限付きサンドボックス環境において、カーネル領域でのコード実行を可能にするカーネル内の仮想マシンです。

仮想マシンには、さまざまな種類のマップの作成を可能にする、新しいシステムコール **bpf()** が含まれ、特別なアセンブリーのコードでプログラムをロードすることも可能です。そして、このコードはカーネルにロードされ、実行時コンパイラーでネイティブマシンコードに変換されます。**bpf()** は、root ユーザーなど、**CAP_SYS_ADMIN** が付与されているユーザーのみが利用できます。詳細は、man ページの **bpf(2)** を参照してください。

ロードしたプログラムは、データを受信して処理するために、さまざまなポイント (ソケット、トレースポイント、パケット受信) に割り当てることができます。

eBPF 仮想マシンを使用する Red Hat には、多くのコンポーネントが同梱されています。各コンポーネントは異なる開発フェーズにあります。特定のコンポーネントがサポート対象と示されていない限り、すべてのコンポーネントはテクノロジープレビューとして提供されます。

現在、以下の主要 **eBPF** コンポーネントが、テクノロジープレビューとして利用可能です。

- **AF_XDP**。これは、**eXpress Data Path (XDP)**パスを、パケット処理のパフォーマンスを優先するアプリケーションのユーザー空間に接続するためのソケットです。

Bugzilla:1559616[1]

kexec fast reboot 機能は、テクノロジープレビューとしてご利用いただけます。

kexec fast reboot 機能は、引き続きテクノロジープレビューとして利用できます。**kexec** 高速リブートでは、最初に基本入出力システム (BIOS) やファームウェアを経由せずに 2 番目のカーネルを直接ブートできるため、ブートプロセスが大幅に高速化されます。この機能を使用するには、以下を実行します。

1. **kexec** カーネルを手動で読み込みます。
2. 変更を有効にするために再起動します。

kexec 高速リブート機能は、RHEL 9 以降のリリースではサポート範囲が限定されていることに注意してください。

Bugzilla:1769727

カーネルの Intel データストリーミングタブレットドライバーがテクノロジープレビューとして利用可能になる

カーネルの Intel データストリーミングアクセラレータードライバー (IDXD) は、現在テクノロジープレビューとして利用できます。これは Intel CPU 統合アクセラレーターで、プロセスアドレス空間 ID (pasid) の送信および共有仮想メモリー (SVM) の共有ワークキューが含まれますます。

Bugzilla:1837187[1]

accel-config パッケージがテクノロジープレビューとして利用可能になりました。

accel-config パッケージが、テクノロジープレビューとして、Intel **EM64T** および **AMD64** アーキテクチャーで利用可能になりました。このパッケージは、Linux カーネルでデータストリーミング (DSA) サブシステムを制御し、設定するのに役立ちます。また、**sysfs** (pseudo-filesystem) を介してデバイスを設定し、設定を **json** 形式で保存および読み込みます。

Bugzilla:1843266[1]

SGX がテクノロジープレビューとして利用可能

Software Guard Extensions(SGX) は、ソフトウェアコードおよび公開および修正からのデータを保護する Intel® テクノロジーです。RHEL カーネルは、SGX v1 および v1.5 の機能を部分的に提供します。バージョン 1 では、**Flexible Launch Control** メカニズムを使用するプラットフォームで SGX テクノロジーを使用できるようになります。バージョン 2 では、**Enclave Dynamic Memory Management** (EDMM) が追加されています。主な変更には以下のものがあります。

- 初期化されたエンクレーブに属する通常のエンクレーブページの EPCM 権限を変更します。
- 初期化されたエンクレーブへの通常のエンクレーブページを動的追加しました。
- より多くのスレッドを収容できるように初期化されたエンクレーブを拡張します。
- 初期化されたエンクレーブから通常のページと TCS ページを削除します。

Bugzilla:1660337[1]

9.4. ファイルシステムおよびストレージ

ファイルシステム DAX が、テクノロジープレビューとして ext4 および XFS で利用可能に

Red Hat Enterprise Linux 8 では、ファイルシステムの DAX がテクノロジープレビューとして利用できます。DAX は、永続メモリーをそのアドレス空間に直接マッピングする手段をアプリケーションに提供します。DAX を使用するには、システムで利用可能な永続メモリーの形式が必要になります。通常は、NVDIMM (Non-Volatile Dual In-line Memory Module) の形式で、DAX 機能を提供するファイルシステムを NVDIMM に作成する必要があります。また、ファイルシステムは **dax** マウントオプションでマウントする必要があります。これにより、dax をマウントしたファイルシステムのファイルの **mmap** が、アプリケーションのアドレス空間にストレージを直接マッピングされます。

Bugzilla:1627455[1]

OverlayFS

OverlayFS は、ユニオンファイルシステムのタイプです。これにより、あるファイルシステムを別のファイルシステムに重ねることができます。変更は上位のファイルシステムに記録され、下位のファイルシステムは変更しません。これにより、ベースイメージが読み取り専用メディアにあるコンテナーや DVD-ROM などのファイルシステムイメージを、複数のユーザーが共有できるようになります。

OverlayFS は、ほとんどの状況で引き続きテクノロジープレビューになります。したがって、カーネルは、この技術がアクティブになると警告を記録します。

以下の制限下で、対応しているコンテナーエンジン (**podman**、**cri-o**、または **buildah**) とともに使用すると、OverlayFS に完全対応となります。

- OverlayFS は、コンテナーエンジングラフドライバーとしての使用、または圧縮された **kdump** initramfs などのその他の特殊なユースケースとしての使用のみサポートされています。その使用は主にコンテナー COW コンテンツでサポートされており、永続ストレージではサポートされていません。非 OverlayFS ボリュームに永続ストレージを配置する必要があります。デフォルトのコンテナーエンジン設定のみを使用できます。つまり、あるレベルのオーバーレイ、1 つの下位ディレクトリー、および下位と上位の両方のレベルが同じファイルシステムにあります。
- 下層ファイルシステムとして使用に対応しているのは現在 XFS のみです。

また、OverlayFS の使用には、以下のルールと制限が適用されます。

- OverlayFS カーネル ABI とユーザー空間の動作については安定しているとみなされていないため、今後の更新で変更が加えられる可能性があります。
- OverlayFS は、POSIX 標準の制限セットを提供します。OverlayFS を使用してアプリケーションをデプロイする前に、アプリケーションを十分にテストしてください。以下のケースは、POSIX に準拠していません。
  - **O_RDONLY** で開いているファイルが少ない場合は、ファイルの読み取り時に **st_atime** の更新を受け取りません。
  - **O_RDONLY** で開いてから、**MAP_SHARED** でマッピングした下位ファイルは、後続の変更と一貫性がありません。
  - 完全に準拠した **st_ino** 値または **d_ino** 値は、RHEL 8 ではデフォルトで有効になっていませんが、モジュールオプションまたはマウントオプションを使用して、この値の完全な POSIX コンプライアンスを有効にできます。
    一貫した inode 番号を付けるには、**xino=on** マウントオプションを使用します。

    redirect_dir=on オプションおよび **index=on** オプションを使用して、POSIX コンプライアンスを向上させることもできます。この 2 つのオプションにより、上位レイヤーの形式は、このオプションなしでオーバーレイと互換性がありません。つまり、**redirect_dir=on** または **index=on** でオーバーレイを作成し、オーバーレイをアンマウントしてから、このオプションなしでオーバーレイをマウントすると、予期しない結果またはエラーが発生することがあります。
- 既存の XFS ファイルシステムがオーバーレイとして使用できるかどうかを確認するには、次のコマンドを実行して、**ftype=1** オプションが有効になっているかどうかを確認します。

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

- SELinux セキュリティーラベルは、OverlayFS で対応するすべてのコンテナーエンジンでデフォルトで有効になっています。
- このリリースの既知の問題は、OverlayFS に関連しています。詳細は **Linux カーネルドキュメント** の Non-standard behavior を参照してください。

OverlayFS の詳細は、Linux カーネルのドキュメント を参照してください。

Bugzilla:1690207[1]

Straits がテクノロジープレビューとして利用可能になりました。

Stratis は、追加機能を備えたストレージプール上に管理されたファイルシステムを提供する、新しいローカルストレージマネージャーです。これはテクノロジープレビューとして提供されます。

Stratis を使用すると、次のストレージタスクを実行できます。

- スナップショットおよびシンプロビジョニングを管理する
- 必要に応じてファイルシステムのサイズを自動的に大きくする
- ファイルシステムを維持する

Stratis ストレージを管理するには、バックグランドサービス **stratisd** と通信する **stratis** ユーティリティーを使用します。詳細は、Stratis ファイルシステムのセットアップ ドキュメントを参照してください。

RHEL 8.5 は Stratis をバージョン 2.42 に更新した。詳細は、Stratis 2.4.2 リリースノート を参照してください。

Jira:RHELPLAN-1212[1]

NVMe/TCP ホストはテクノロジープレビューとして利用可能です

TCP/IP ネットワーク (NVMe/TCP) および対応する **nvme-tcp.ko** カーネルモジュールへのアクセスおよび共有がテクノロジープレビューとして追加されました。ホストとしての NVMe/TCP の使用は、**nvme-cli** パッケージによって提供されるツールを使用して管理できます。NVMe/TCP ホストテクノロジープレビュー機能はテスト目的としてのみ同梱されており、現時点ではフルサポートの予定はありません。

Bugzilla:1696451[1]

テクノロジープレビューとして、IdM ドメインメンバーで Samba サーバーを設定できるようになりました。

今回の更新で、Identity Management (IdM) ドメインメンバーに Samba サーバーを設定できるようになりました。同じ名前パッケージに含まれる新しい **ipa-client-samba** ユーティリティーは、Samba 固有の Kerberos サービスプリンシパルを IdM に追加し、IdM クライアントを準備します。たとえば、ユーティリティーは、**sss** ID マッピングバックエンドの ID マッピング設定で **/etc/samba/smb.conf** を作成します。その結果、管理者が IdM ドメインメンバーに Samba を設定できるようになりました。

IdM 信頼コントローラーが Global Catalog Service をサポートしないため、AD が登録した Windows ホストは Windows で IdM ユーザーおよびグループを見つけることができません。さらに、IdM 信頼コントローラーは、Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) プロトコルを使用する IdM グループの解決をサポートしません。これにより、AD ユーザーは、IdM クライアントから Samba の共有およびプリンターにしかアクセスできません。

詳細は、IdM ドメインメンバーでの Samba の設定 を参照してください。

Jira:RHELPLAN-13195[1]

9.5. 高可用性およびクラスター

Pacemaker の podman バンドルがテクノロジープレビューとして利用可能になりました。

Pacemaker コンテナーバンドルは、テクノロジープレビューとして利用できるコンテナーバンドル機能を使用して、Podman で動作するようになりました。この機能はテクノロジープレビューとして利用できますが、例外が 1 つあります。Red Hat は、Red Hat OpenStack 用の Pacemaker バンドルの使用に完全対応します。

Bugzilla:1619620[1]

テクノロジープレビューとして利用可能な corosync-qdevice のヒューリスティック

ヒューリスティックは、起動、クラスターメンバーシップの変更、**corosync-qnetd** への正常な接続でローカルに実行され、任意で定期的に実行される一連のコマンドです。すべてのコマンドが時間どおりに正常に終了すると (返されるエラーコードがゼロである場合)、ヒューリスティックは渡されますが、それ以外の場合は失敗します。ヒューリスティックの結果は **corosync-qnetd** に送信され、クオーラムとなるべきパーティションを判断するための計算に使用されます。

Bugzilla:1784200

新しい fence-agents-heuristics-ping フェンスエージェント

Pacemaker は、テクノロジープレビューとして **fence_heuristics_ping** エージェントを提供するようになりました。このエージェントの目的は、実際にはフェンシングを行わず、フェンシングレベルの動作を新しい方法で活用する実験的なフェンスエージェントのクラスを開くことです。

ヒューリスティックエージェントが、実際のフェンシングを行うフェンスエージェントと同じフェンシングレベルで設定されいて、そのエージェントよりも順番が前に設定されているとします。その場合、フェンシグを行うエージェントで **off** 操作を行う前に、ヒューリスティックエージェントで、この操作を行います。このヒューリスティックエージェントが **off** アクションに対して失敗する場合、このフェンシングレベルが成功しないのはすでに明らかです。そのため、Pacemaker フェンシングは、フェンシングを行うエージェントで **off** 操作を行うステップをスキップします。ヒューリスティックエージェントはこの動作を利用して、特定の条件下で、実際のフェンシングを行うエージェントがフェンシングできないようにできます。

サービスを適切に引き継ぐことができないことを事前に把握できる場合は、ノードがピアをフェンシングする意味がないのであれば、ユーザーは特に 2 ノードクラスターでこのエージェントを使用できます。たとえば、ネットワークアップリンクに到達してサービスがクライアントに到達できない場合は、ノードがサービスを引き継ぐ意味はありません。これは、ルーターへの ping が検出できる状況が考えられます。

Bugzilla:1775847[1]

9.6. IDENTITY MANAGEMENT

Identity Management JSON-RPC API がテクノロジープレビューとして利用可能になりました。

Identity Management (IdM) では API が利用できます。API を表示するために、IdM は、テクノロジープレビューとして API ブラウザーも提供します。

以前では、複数のバージョンの API コマンドを有効にするために、IdM API が拡張されました。これらの機能拡張により、互換性のない方法でコマンドの動作が変更することがありました。IdM API を変更しても、既存のツールおよびスクリプトを引き続き使用できるようになりました。これにより、以下が可能になります。

- 管理者は、管理しているクライアント以外のサーバーで、IdM の以前のバージョンもしくは最近のバージョンを使用できます。
- サーバーで IdM のバージョンを変更しても、開発者は特定バージョンの IdM コールを使用できます。

すべてのケースでサーバーとの通信が可能になります。たとえば、ある機能向けの新オプションが新しいバージョンに追加されていて、通信の一方の側でこれを使用していたとしても、特に問題はありません。

API の使用方法は Identity Management API を使用して IdM サーバーに接続する (テクノロジープレビュー) を参照してください。

Bugzilla:1664719

DNSSEC が IdM でテクノロジープレビューとして利用可能

統合 DNS のある Identity Management (IdM) サーバーは、DNS プロトコルのセキュリティーを強化する DNS に対する拡張セットである DNS Security Extensions (DNSSEC) を実装するようになりました。IdM サーバーでホストされる DNS ゾーンは、DNSSEC を使用して自動的に署名できます。暗号鍵は、自動的に生成およびローテートされます。

DNSSEC で DNS ゾーンを保護する場合は、以下のドキュメントを参照することが推奨されます。

- DNSSEC Operational Practices, Version 2
- Secure Domain Name System (DNS) Deployment Guide
- DNSSEC Key Rollover Timing Considerations

統合 DNS のある IdM サーバーは、DNSSEC を使用して、他の DNS サーバーから取得した DNS 回答を検証することに注意してください。これが、推奨される命名方法に従って設定されていない DNS ゾーンの可用性に影響を与える可能性があります。

Bugzilla:1664718

ACME がテクノロジープレビューとして利用可能

Automated Certificate Management Environment (ACME) サービスが、テクノロジープレビューとして Identity Management (IdM) で利用可能になりました。ACME は、自動化識別子の検証および証明書の発行に使用するプロトコルです。この目的は、証明書の有効期間を短縮し、証明書のライフサイクル管理での手動プロセスを回避することにより、セキュリティーを向上させることです。

RHEL では、ACME サービスは Red Hat Certificate System (RHCS) PKI ACME レスポンダーを使用します。RHCS ACME サブシステムは、IdM デプロイメントのすべての認証局 (CA) サーバーに自動的にデプロイされますが、管理者が有効にするまでリクエストに対応しません。RHCS は、ACME 証明書を発行する際に **acmeIPAServerCert** プロファイルを使用します。発行された証明書の有効期間は 90 日です。ACME サービスの有効化または無効化は、IdM デプロイメント全体に影響します。

重要

ACME は、すべてのサーバーが RHEL 8.4 以降を実行している IdM デプロイメントでのみ有効にすることが推奨されます。以前の RHEL バージョンには ACME サービスが含まれていないため、バージョンが混在するデプロイメントで問題が発生する可能性があります。たとえば、ACME のない CA サーバーは、異なる DNS サブジェクト代替名 (SAN) を使用しているため、クライアント接続が失敗する可能性があります。

警告

現在、RHCS は期限切れの証明書を削除しません。ACME 証明書は 90 日後に期限切れになるため、期限切れの証明書が蓄積され、パフォーマンスに影響を及ぼす可能性があります。

- IdM デプロイメント全体で ACME を有効にするには、**ipa-acme-manage enable** コマンドを使用します。

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

- IdM デプロイメント全体で ACME を無効にするには、**ipa-acme-manage disable** コマンドを使用します。

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

- ACME サービスがインストールされ、有効または無効であるかを確認するには、**ipa-acme-manage status** コマンドを使用します。

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

Bugzilla:1628987[1]

sssd-idp サブパッケージがテクノロジープレビューとして利用可能

SSSD の **sssd-idp** サブパッケージには、Identity Management (IdM) サーバーに対して OAuth2 認証を実行するクライアント側のコンポーネントである **oidc_child** プラグインおよび krb5 **idp** プラグインが含まれます。この機能は、RHEL 8.7 以降の IdM サーバーのみで使用できます。

Bugzilla:2065692

SSSD の内部 krb5 idp プラグインがテクノロジープレビューとして利用可能

SSSD krb5 **idp** プラグインを使用すると、OAuth2 プロトコルを使用して外部アイデンティティープロバイダー (IdP) に対して認証できます。この機能は、RHEL 8.7 以降の IdM サーバーのみで使用できます。

Bugzilla:2056483

RHEL IdM では、ユーザー認証をテクノロジープレビューとして外部 ID プロバイダーに委任できる

RHEL IdM のテクノロジープレビューとして、OAuth 2 デバイス認証フローをサポートする外部アイデンティティプロバイダー (IdP) にユーザーを関連付けられるようになりました。これらのユーザーが RHEL 8.7 以降で利用可能な SSSD バージョンで認証すると、外部 IdP で認証と認可を実行した後、Kerberos チケットを使用した RHEL IdMSingle Sign-On 機能を受け取ります。

主な変更には以下のものがあります。

- **ipa idp-*** コマンドによる外部 IdP への参照の追加、変更、および削除
- **ipa user-mod --user-auth-type=idp** コマンドを使用したユーザーの IdP 認証の有効化

追加情報は、外部 ID プロバイダーを使用した IdM への認証 を参照してください。

Bugzilla:2101770

9.7. デスクトップ

64 ビット ARM アーキテクチャーの GNOME がテクノロジープレビューとして利用できるようになりました。

GNOME デスクトップ環境は、テクノロジープレビューとして 64 ビット ARM アーキテクチャーで利用できます。

VNC を使用して 64 ビット ARM サーバーのデスクトップセッションに接続できるようになりました。その結果、グラフィカルアプリケーションを使用してサーバーを管理できます。

64 ビット ARM では、限定されたグラフィカルアプリケーションのセットを使用できます。以下に例を示します。

- Firefox Web ブラウザー
- Red Hat Subscription マネージャー (**subscription-manager-cockpit**)
- ファイアウォール設定 (**firewall-config**)
- ディスク使用状況アナライザー (**baobab**)

Firefox を使用して、サーバー上の Cockpit サービスに接続できます。

LibreOffice などの特定のアプリケーションは、コマンドラインインターフェイスのみを提供し、グラフィカルインターフェイスは無効になっています。

Jira:RHELPLAN-27394[1]、Bugzilla:1667225、Bugzilla:1724302、Bugzilla:1667516

テクノロジープレビューとして利用可能な IBM Z アーキテクチャー用の GNOME

GNOME デスクトップ環境は、テクノロジープレビューとして IBM Z アーキテクチャーで利用できます。

VNC を使用して IBM Z サーバーのデスクトップセッションに接続できるようになりました。その結果、グラフィカルアプリケーションを使用してサーバーを管理できます。

IBM Z では、限定されたグラフィカルアプリケーションのセットを使用できます。たとえば、次のようになります。

- Firefox Web ブラウザー
- Red Hat Subscription マネージャー (**subscription-manager-cockpit**)
- ファイアウォール設定 (**firewall-config**)
- ディスク使用状況アナライザー (**baobab**)

Firefox を使用して、サーバー上の Cockpit サービスに接続できます。

LibreOffice などの特定のアプリケーションは、コマンドラインインターフェイスのみを提供し、グラフィカルインターフェイスは無効になっています。

Jira:RHELPLAN-27737[1]

9.8. グラフィックインフラストラクチャー

64 ビット ARM アーキテクチャーで VNC リモートコンソールがテクノロジープレビューとして利用可能に

64 ビットの ARM アーキテクチャーでは、Virtual Network Computing (VNC) リモートコンソールがテクノロジープレビューとして利用できます。グラフィックススタックの残りの部分は、現在、64 ビット ARM アーキテクチャーでは検証されていません。

Bugzilla:1698565[1]

9.9. 仮想化

RHEL 8 Hyper-V 仮想マシンで KVM 仮想化が利用可能に

ネストされた KVM 仮想化は、テクノロジープレビューとして、Microsoft Hyper-V ハイパーバイザーで使用できるようになりました。これにより、Hyper-V ホストで実行している RHEL 8 ゲストシステムで仮想マシンを作成できます。

この機能は、現在 Intel および AMD システムでのみ有効です。また、ネストされた仮想化は、Hyper-V でデフォルトで有効になっていない場合があります。これを有効にするには、以下の Microsoft ドキュメントを参照してください。

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

Bugzilla:1519039[1]

KVM 仮想マシンの AMD SEV および SEV-ES

テクノロジープレビューとして、RHEL 8 に、KVM ハイパーバイザーを使用する AMD EPYC ホストマシン用のセキュア暗号化仮想化 (SEV) 機能が同梱されます。仮想マシンで有効になっている場合は、SEV が仮想マシンのメモリーを暗号化して、ホストから仮想マシンへのアクセスを防ぎます。これにより、仮想マシンのセキュリティーが向上します。

さらに、強化された SEV (Encrypted State) バージョンの SEV (SEV-ES) もテクノロジープレビューとして提供されます。SEV-ES は、仮想マシンの実行が停止すると、すべての CPU レジスターの内容を暗号化します。これにより、ホストが仮想マシンの CPU レジスターを変更したり、そこから情報を読み取ったりできなくなります。

SEV および SEV-ES は、第 2 世代の AMD EPYC CPU (コードネーム Rome) 以降でのみ機能することに注意してください。また、RHEL 8 には SEV および SEV-ES の暗号化が含まれますが、SEV および SEV-ES のセキュリティー証明は含まれません。

Bugzilla:1501618[1]、Jira:RHELPLAN-7677、Bugzilla:1501607

Intel vGPU がテクノロジープレビューとして利用可能になる

テクノロジープレビューとして、物理 Intel GPU デバイスを、**mediated devices** と呼ばれる複数の仮想デバイスに分割できるようになりました。この仲介デバイスは、仮想 GPU として複数の仮想マシンに割り当てることができます。これにより、この仮想マシンが、1 つの物理 Intel GPU のパフォーマンスを共有します。

選択した Intel GPU のみが vGPU 機能と互換性があることに注意してください。

さらに、Intel vGPU が操作する VNC コンソールを有効にすることもできます。これを有効にすると、ユーザーは仮想マシンの VNC コンソールに接続し、Intel vGPU がホストする仮想マシンのデスクトップを確認できます。ただし、これは現在 RHEL ゲストオペレーティングシステムでのみ動作します。

この機能は非推奨であり、今後の RHEL メジャーリリースでは完全に削除される予定であることに注意してください。

Bugzilla:1528684[1]

入れ子仮想マシンの作成

入れ子 KVM 仮想化は、RHEL 8 で Intel、AMD64、IBM POWER および IBM Z システムホストで実行している KVM 仮想マシン用のテクノロジープレビューとして提供されます。この機能を使用すると、物理 RHEL 8 ホストで実行中の RHEL 7 または RHEL 8 仮想マシンがハイパーバイザーとして機能し、独自の仮想マシンをホストできます。

Jira:RHELPLAN-14047[1]、Jira:RHELPLAN-24437

テクノロジープレビュー: 一部の Intel ネットワークアダプターが、Hyper-V の RHEL ゲストに SR-IOV を提供するようになりました

テクノロジープレビューとして、Hyper-V ハイパーバイザーで実行している Red Hat Enterprise Linux のゲストオペレーティングシステムは、**ixgbevf** および **ixgbevf** ドライバーがサポートする Intel ネットワークアダプターに、シングルルート I/O 仮想化 (SR-IOV) 機能を使用することができるようになりました。この機能は、以下の条件が満たされると有効になります。

- ネットワークインターフェイスコントローラー (NIC) に対して SR-IOV サポートが有効になっている
- 仮想 NIC の SR-IOV サポートが有効になっている
- 仮想スイッチの SR-IOV サポートが有効になっている
- NIC からの VF (Virtual Function) が仮想マシンに割り当てられている

この機能は現在、Microsoft Windows Server 2016 以降で提供されています。

Bugzilla:1348508[1]

RHEL ゲストのインテル TDX

テクノロジープレビューとして、Intel Trust Domain Extension (TDX) 機能が RHEL 8.8 以降のゲストオペレーティングシステムで使用できるようになりました。ホストシステムが TDX をサポートしている場合は、トラストドメイン (TD) と呼ばれる、ハードウェアから分離された RHEL 9 仮想マシン (VM) をデプロイできます。ただし、TDX は現在 **kdump** では機能せず、TDX を有効にすると VM 上で **kdump** が失敗することに注意してください。

Bugzilla:1836977[1]

virtiofs を使用したホストと仮想マシン間でのファイルの共有

RHEL 8 では、テクノロジープレビューとして virtio ファイルシステム (**virtiofs**) が追加されました。**virtiofs** を使用すると、ホストシステムと仮想マシン (VM) との間で、ファイルを効率的に共有できます。

Bugzilla:1741615[1]

9.10. クラウド環境の RHEL

RHEL Confidential VMs がテクノロジープレビューとして Azure で利用可能になりました

更新された RHEL カーネルを使用すると、Microsoft Azure で機密仮想マシン (VM) をテクノロジープレビューとして作成して実行できるようになりました。ただし、Azure での起動中に RHEL 機密 VM イメージを暗号化することはまだできません。

Jira:RHELPLAN-122316[1]

9.11. コンテナー

Podman の SQLite データベースバックエンドがテクノロジープレビューとして利用可能

Podman v4.6 以降、Podman の SQLite データベースバックエンドはテクノロジープレビューとして利用可能です。データベースバックエンドを SQLite に設定するには、**/etc/containers/containers.conf** 設定ファイルに **database_backend = "sqlite"** オプションを追加します。SQLite データベースバック

エンドに切り替える前に、**podman system reset** コマンドを実行してストレージを初期状態にリセットします。すべてのコンテナーと Pod を再作成する必要があることに注意してください。SQLite データベースは、優れた安定性と一貫性を保証します。コンテナースタック内の他のデータベースも同様に SQLite に移動されます。BoltDB は引き続きデフォルトのデータベースバックエンドです。

Jira:RHELPLAN-154428[1]

podman-machine コマンドはサポート対象外です。

仮想マシンを管理するための **podman-machine** コマンドは、テクノロジープレビューとしてのみ利用可能です。代わりに、コマンドラインから直接 Podman を実行してください。

Jira:RHELDOCS-16861[1]

第10章 非推奨になった機能

ここでは、Red Hat Enterprise Linux 8 で **非推奨** となった機能の概要を説明します。

非推奨の機能は、本製品の今後のメジャーリリースではサポートされない可能性が高く、新たに実装することは推奨されません。特定のメジャーリリースにおける非推奨機能の最新情報は、そのメジャーリリースの最新版のリリースノートを参照してください。

非推奨機能のサポートステータスは、Red Hat Enterprise Linux 8 では変更されません。サポート期間の詳細は、Red Hat Enterprise Linux ライフサイクル および Red Hat Enterprise Linux Application Streams ライフサイクル を参照してください。

現行および今後のメジャーリリースでは、非推奨のハードウェアコンポーネントの新規実装は推奨されません。ハードウェアドライバーの更新は、セキュリティーと重大な修正のみに行われます。Red Hat では、このようなハードウェアの早期交換を推奨します。

パッケージが非推奨となり、使用の継続が推奨されない場合があります。製品からパッケージが削除されることもあります。その場合には、製品のドキュメントで、非推奨となったパッケージと同様、同一、またはより高度な機能を提供する最近のパッケージが指定され、詳しい推奨事項が記載されます。

RHEL 7 で使用され、RHEL 8 で **削除された** 機能の詳細は RHEL 8 の導入における検討事項 を参照してください。

10.1. インストーラーおよびイメージの作成

複数のキックスタートコマンドおよびオプションが非推奨になりました。

RHEL 8 キックスタートファイルで以下のコマンドとオプションを使用すると、ログに警告が表示されます。

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

特定のオプションだけがリスト表示されている場合は、基本コマンドおよびその他のオプションは引き続き利用でき、非推奨ではありません。

キックスタートの詳細および変更点は、**RHEL 8 の導入における検討事項**の キックスタートの変更 を参照してください。

Bugzilla:1642765[1]

キックスタートコマンド ignoredisk の --interactive オプションが非推奨になりました。

Red Hat Enterprise Linux の将来のリリースで **--interactive オプション** を使用すると、致命的なインストールエラーが発生します。このオプションを削除するには、キックスタートファイルを変更することが推奨されます。

Bugzilla:1637872[1]

キックスタートの autostep コマンドが非推奨に

autostep コマンドが非推奨になりました。このコマンドに関連するセクションは、RHEL 8 のドキュメント から削除されました。

Bugzilla:1904251[1]

10.2. セキュリティー

NSS SEED 暗号が非推奨になりました。

Mozilla Network Security Services (**NSS**) ライブラリーでは、今後のリリースで SEED 暗号化を使用する TLS 暗号スイートのサポートがなくなります。NSS がサポートを削除した際に SEED 暗号に依存するデプロイメントを円滑に移行させるため、Red Hat は、他の暗号スイートのサポートを有効にすることを推奨します。

RHEL では、SEED 暗号はデフォルトですでに無効にされています。

Bugzilla:1817533

TLS 1.0 および TLS 1.1 が非推奨になりました。

TLS 1.0 プロトコルおよび TLS 1.1 プロトコルは、システム全体の暗号化ポリシーレベル **DEFAULT** で無効になります。たとえば、Firefox Web ブラウザーのビデオ会議アプリケーションで、非推奨のプロトコルを使用する必要がある場合は、システム全体の暗号化ポリシーを **LEGACY** レベルに変更してください。

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

詳細は、Red Hat カスタマーポータルのナレッジベースの記事 Strong crypto defaults in RHEL 8 and deprecation of weak crypto algorithms および man ページの **update-crypto-policies(8)** を参照してください。

Bugzilla:1660839

RHEL 8 で DSA が非推奨になりました。

デジタル署名アルゴリズム (DSA) は、Red Hat Enterprise Linux 8 では非推奨であると考えられています。DSA キーに依存する認証メカニズムはデフォルト設定では機能しません。**OpenSSH** クライアントは、**LEGACY** のシステム全体の暗号化ポリシーレベルでも DSA ホストキーを許可しません。

Bugzilla:1646541[1]

fapolicyd.rules が非推奨になる

実行ルールの許可と拒否を含むファイルの **/etc/fapolicyd/rules.d/** ディレクトリーは、**/etc/fapolicyd/fapolicyd.rules** ファイルを置き換えます。**fagenrules** スクリプトは、このディレクトリー内のすべてのコンポーネントルールファイルを **/etc/fapolicyd/compiled.rules** ファイルにマージするようになりました。**/etc/fapolicyd/fapolicyd.trust** のルールは引き続き **fapolicyd** フレームワークによって処理されますが、下位互換性を確保するためのみに使用されます。

Bugzilla:2054741

NSS で SSL2 Client Hello が非推奨に

TLS (Transport Layer Security) プロトコルバージョン 1.2 以前は、 **SSL** (Secure Sockets Layer) プロトコルバージョン 2 と後方互換性がある形式の **Client Hello** メッセージを使用してネゴシエーションを開始できます。**NSS** (Network Security Services) ライブラリーでのこの機能への対応は非推奨となっており、デフォルトで無効になっています。

この機能への対応が必要なアプリケーションを有効にするには、新しい API の **SSL_ENABLE_V2_COMPATIBLE_HELLO** を使用する必要があります。この機能への対応は、Red Hat Enterprise Linux 8 の将来のリリースから完全に削除される可能性があります。

Bugzilla:1645153[1]

NTLM と Krb4 は Cyrus SASL では非推奨となりました。

NTLM および Kerberos 4 認証プロトコルは非推奨となり、RHEL の今後のメジャーバージョンでは削除される可能性があります。これらのプロトコルはセキュアであると見なされなくなり、アップストリームの実装からはすでに削除されています。

Jira:RHELDOCS-17380[1]

/etc/selinux/config を使用して SELinux を無効にするランタイムが非推奨になりました。

/etc/selinux/config ファイルの **SELINUX=disabled** オプションを使用して SELinux を無効にするランタイムが非推奨になりました。RHEL 9 では、**/etc/selinux/config** でのみ SELinux を無効にすると、システムは SELinux が有効化されますが、ポリシーが読み込まれずに開始します。

SELinux を完全に無効にする必要がある場合には、Red Hat は、**selinux=0** パラメーターをカーネルコマンドラインに追加して SELinux を無効にすることを推奨します。これは、SELinux の使用 タイトルの システムの起動時に SELinux モードの変更 セクションで説明されています。

Bugzilla:1932222

selinux-policy から ipa SELinux モジュールが削除されました。

ipa SELinux はメンテナンスされなくなったため、**selinux-policy** から削除されました。この機能は、**ipa-selinux** サブパッケージに含まれるようになりました。

ローカルの SELinux ポリシーで、**ipa** モジュールからタイプやインターフェイスを使用する必要がある場合は、**ipa-selinux** をインストールします。

Bugzilla:1461914[1]

TPM 1.2 が非推奨になりました。

Trusted Platform Module (TPM) のセキュアな暗号化プロセッサーの標準バージョンが 2016 年に バー

ジョン 2.0 に更新されました。TPM 2.0 は TPM 1.2 に対する多くの改良を提供しますが、以前のバージョンと後方互換性はありません。TPM 1.2 は RHEL 8 で非推奨となり、次のメジャーリリースで削除される可能性があります。

Bugzilla:1657927[1]

crypto-policies から派生したプロパティーが非推奨に

カスタムポリシーにおける **crypto-policies** ディレクティブのスコープの導入により、**tls_cipher**、**ssh_cipher**、**ssh_group**、**ike_protocol**、および **sha1_in_dnssec** の派生プロパティーが非推奨になりました。さらに、スコープを指定しない **protocol** プロパティーの使用も非推奨になりました。推奨される代替は、**crypto-policies(7)** の man ページを参照してください。

Bugzilla:2011208

10.3. サブスクリプションの管理

subscription-manager コマンドの --token オプションは非推奨になりました。

subscription-manager register コマンドの **--token=<TOKEN>** オプションは、システムを Red Hat に登録するのに役立つ認証方法です。このオプションは、エンタイトルメントサーバーが提供する機能に応じて異なります。デフォルトのエンタイトルメントサーバー **subscription.rhsm.redhat.com** は、この機能をオフにする予定です。その結果、**subscription-manager register --token=<TOKEN>** を使用しようとすると、次のエラーメッセージが表示されて失敗する可能性があります。

```
Token authentication not supported by the entitlement server
```

subscription-manager register コマンドのペアのオプション **--username** / **--password** および **--org** / **--activationkey** を含めるなど、他の認証方法を使用してシステムの登録を続けることができます。

Bugzilla:2170082

10.4. ソフトウェア管理

rpmbuild --sign が非推奨になりました。

rpmbuild --sign コマンドは、RHEL 8.1 以降非推奨になりました。Red Hat Enterprise Linux の今後のリリースでこのコマンドを実行すると、エラーが発生します。代わりに **rpmsign** コマンドを使用することが推奨されます。

Bugzilla:1688849

10.5. シェルおよびコマンドラインツール

OpenEXR コンポーネントが非推奨になりました。

OpenEXR コンポーネントが非推奨になりました。そのため、**EXR** イメージ形式のサポートは **imagecodecs** モジュールから削除されました。

Bugzilla:1886310

dump からの dump ユーティリティーが非推奨になりました。

ファイルシステムのバックアップに使用される **dump** ユーティリティーが非推奨になり、RHEL 9 では使用できなくなります。

RHEL 9 では、使用方法に基づいて、**tar**、**dd**、または **bacula** のバックアップユーティリティーを使用することが推奨されています。これにより、ext2、ext3、および ext4 のファイルシステムで完全で安全なバックアップが提供されます。

dump パッケージの **restore** ユーティリティーは、RHEL 9 で引き続き利用可能で、サポートされており、**restore** パッケージとして利用できます。

Bugzilla:1997366[1]

hidepid=n マウントオプションが、RHEL 8 systemd で未サポート

マウントオプションの **hidepid=n** は、**/proc/[pid]** ディレクトリーの情報にアクセスできるユーザーを制御しますが、RHEL 8 で提供されている **systemd** インフラストラクチャーと互換性がありません。

また、このオプションを使用すると、**systemd** が起動する特定のサービスで SELinux の AVC 拒否メッセージが生成され、その他の操作が完了しないようにする場合があります。

詳細は、関連するナレッジベースのソリューション記事 Is mounting /proc with "hidepid=2" recommended with RHEL7 and RHEL8? を参照してください。

Bugzilla:2038929

/usr/lib/udev/rename_device ユーティリティーは非推奨になる

ネットワークインターフェイスの名前を変更するための **udev** ヘルパーユーティリティー **/usr/lib/udev/rename_device** は非推奨になる

Bugzilla:1875485

ABRT ツールは非推奨になりました

アプリケーションのクラッシュを検出して報告するための自動バグ報告ツール (ABRT) は、RHEL8 で非推奨になりました。代わりに、**systemd-coredump** ツールを使用して、プログラムのクラッシュ後に自動的に生成されるファイルであるコアダンプをログに記録して保存します。

Bugzilla:2055826[1]

ReaR crontab は非推奨になりました

rear パッケージの **/etc/cron.d/rear** は RHEL 8 で非推奨になり、RHEL 9 では使用できなくなります。crontab は、ディスクレイアウトが変更されたかどうかを毎晩チェックし、変更が発生した場合は **rear mkrescue** コマンドを実行します。

この機能が必要な場合は、RHEL 9 にアップグレードした後、ReaR の定期的な実行を手動で設定してください。

Bugzilla:2083301

Bacula の SQLite データベースバックエンドは廃止されました

Bacula バックアップシステムは、複数のデータベースバックエンド (PostgreSQL、MySQL、および SQLite) をサポートしていました。SQLite バックエンドは廃止され、RHEL の今後のリリースではサポートされなくなります。代わりに、他のバックエンド (PostgreSQL または MySQL) のいずれかに移行し、新しい展開では SQLite バックエンドを使用しないでください。

Jira:RHEL-6859

raw コマンドは廃止されました

raw (**/usr/bin/raw**) コマンドは廃止されました。Red Hat Enterprise Linux の今後のリリースでこのコマンドを実行すると、エラーが発生します。

Jira:RHELPLAN-133171[1]

10.6. ネットワーク

PF_KEYv2 カーネル API が非推奨になりました

アプリケーションは、**PV_KEYv2** および新しい **netlink** API を使用して、カーネルの IPsec 実装を設定できます。**PV_KEYv2** はアップストリームで積極的に保守されておらず、最新の暗号、オフロード、拡張シーケンス番号サポートなどの重要なセキュリティー機能が欠けています。そのため、RHEL 8.9 以降、**PV_KEYv2** API は非推奨になりました。アプリケーションでこのカーネル API を使用する場合は、代替として最新の **netlink** API を使用するように移行してください。

Jira:RHEL-1257[1]

RHEL 8 でネットワークスクリプトが非推奨に

Red Hat Enterprise Linux 8 では、ネットワークスクリプトが非推奨になっており、デフォルトでは提供されなくなりました。基本的なインストールでは、**nmcli** ツール経由で、NetworkManager サービスを呼び出す **ifup** スクリプトおよび **ifdown** スクリプトの新しいバージョンが提供されます。Red Hat Enterprise Linux 8 で **ifup** スクリプトおよび **ifdown** スクリプトを実行する場合は、NetworkManager を実行する必要があります。

/sbin/ifup-local、**ifdown-pre-local**、および **ifdown-local** の各スクリプトでは、カスタムコマンドが実行されません。

このスクリプトが必要な場合は、次のコマンドを使用すれば、システムに非推奨のネットワークスクリプトをインストールできます。

```
# yum install network-scripts
```

ifup スクリプトと **ifdown** スクリプトが、インストールされている従来のネットワークスクリプトにリンクされます。

従来のネットワークスクリプトを呼び出すと、そのスクリプトが非推奨であることを示す警告が表示されます。

Bugzilla:1647725[1]

dropwatch ツールが非推奨に

dropwatch ツールが非推奨になりました。このツールは今後のリリースではサポートされませんので、新規デプロイメントには推奨できません。このパッケージの代わりに、Red Hat は **perf** コマンドラインツールを使用することを推奨します。

perf コマンドラインツールの使用方法の詳細は、Red Hat カスタマーポータルの Getting started with Perf セクションまたは **perf** の man ページを参照してください。

Bugzilla:1929173

xinetd が非推奨に

xinetd サービスが非推奨になり、RHEL 9 では削除される予定です。代わりに **systemd** を使用します。詳細は、xinetd サービスを systemd に変換する方法 を参照してください。

Bugzilla:2009113[1]

cgdcbxd パッケージが非推奨に

コントロールグループデータセンターブリッジング交換デーモン (**cgdcbxd**) は、データセンターのブリッジ (DCB) のネットリンクイベントをモニターし **net_prio control** グループサブシステムを管理するサービスです。RHEL 8.5 以降では、**cgdcbxd** パッケージは非推奨となり、次の RHEL メジャーリリースで削除されます。

Bugzilla:2006665

WEP Wi-Fi 接続方法が非推奨になりました。

安全でない WEP (wired equivalent privacy) の Wi-Fi 接続方法は、RHEL 8 では非推奨となり、RHEL 9.0 では削除されます。安全な Wi-Fi 接続には、Wi-Fi Protected Access 3 (WPA3) または WPA2 の接続方法を使用します。

Bugzilla:2029338

サポートされていない xt_u32 モジュールが非推奨になりました。

サポートされていない **xt_u32** を使用すると、**iptable** のユーザーはパケットヘッダーまたはペイロード内の任意の 32 ビットにマッチできます。RHEL 8.6 以降、**xt_u32** モジュールが非推奨になり、RHEL 9 では削除されます。

xt_u32 を使用する場合は、**nftable** パケットフィルタリングフレームワークに移行します。たとえば、最初にファイアウォールを、個々のルールを段階的に置き換えるために、ネイティブ一致で **iptable** を使用するように変更し、その後に **iptables-translate** と付属のユーティリティーを使用して **nftable** に移行します。**nftable** にネイティブマッチが存在しない場合は、**nftable** の raw ペイロードマッチング機能を使用します。詳細は、**nft(8)** man ページの **raw ペイロード表現** セクションを参照してください。

Bugzilla:2061288

slaves という用語は、nmstate API では非推奨です。

Red Hat では、意識的な言語の使用に取り組んでいます。したがって、**slaves** という用語は Nmstate API では非推奨です。**nmstatectl** を使用する場合は、**port** という用語を使用します。

Jira:RHELDOCS-17641

10.7. カーネル

rdma_rxe Soft-RoCE ドライバーが非推奨に

Remote Software Direct Memory Access over Converged Ethernet (Soft-RoCE) は RXE としても知られており、RDMA (Remote Direct Memory Access) をエミュレートする機能です。RHEL 8 では、Soft-RoCE 機能が、サポートされていないテクノロジープレビューとして利用できます。ただし、安定性の問題により、この機能は非推奨になり、RHEL 9 では削除されます。

Bugzilla:1878207[1]

Linux firewire サブシステムおよび関連するユーザー空間コンポーネントは、RHEL 8 では非推奨になりました。

firewire サブシステムは、IEEE 1394 バスでリソースを使用し、維持するインターフェイスを提供します。RHEL 9 では、**firewire** は、**kernel** パッケージで対応しなくなります。**firewire** には、**libavc1394**、**libdc1394**、**libraw1394** パッケージで提供されるユーザー空間コンポーネントが複数含まれることに注意してください。これらのパッケージも非推奨になります。

Bugzilla:1871863[1]

ディスクレスブートを使用した RHEL for Real Time 8 のインストールが非推奨になりました。

ディスクレスブートにより、複数のシステムがネットワーク経由で root ファイルシステムを共有できます。メリットはありますが、ディスクレスブートでは、リアルタイムのワークロードでネットワークレイテンシーが発生する可能性が高くなります。RHEL for Real Time 8 の将来のマイナー更新では、ディスクレスブート機能はサポートされなくなります。

Bugzilla:1748980

カーネルライブパッチが、すべての RHEL マイナーリリースに対応するようになりました。

RHEL 8.1 以降、カーネルライブパッチは、影響度が重大および重要な Common Vulnerabilities and Exposures (CVE) を修正するために、Extended Update Support (EUS) ポリシーの対象となる RHEL の一部のマイナーリリースストリームに提供されています。同時にカバーされるカーネルとユースケースの最大数に対応するため、各ライブパッチのサポート期間は、カーネルのマイナー、メジャー、および zStream の各バージョンで 12 カ月から 6 カ月に短縮されました。これは、カーネルライブパッチがリリースされると、過去 6 カ月間に配信されたすべてのマイナーリリースとスケジュール済みのエラータカーネルが含まれます。

この機能の詳細は、Applying patches with kernel live patching を参照してください。

利用可能なカーネルライブパッチの詳細は、Kernel Live Patch life cycles を参照してください。

Bugzilla:1958250

crash-ptdump-command パッケージは非推奨です

クラッシュユーティリティーの **ptdump** 拡張モジュールである **crash-ptdump-command** パッケージは非推奨であり、将来の RHEL リリースでは利用できなくなる可能性があります。**ptdump** コマンドは、Single Range Output モードで作業している場合、ログバッファーの取得に失敗し、Table of Physical Addresses (ToPA) モードでのみ機能します。**crash-ptdump-command** は現在、アップストリームに維持されていません

Bugzilla:1838927[1]

10.8. ブートローダー

kernelopts 環境変数は非推奨になる

RHEL 8 では、GRUB ブートローダーを使用するシステムのカーネルコマンドラインパラメーターが **kernelopts** 環境変数で定義されていました。変数は、カーネルブートエントリーごとに **/boot/grub2/grubenv** ファイルに保存されました。ただし、**kernelopts** を使用してカーネルコマンドラインパラメーターを保存することは堅牢ではありませんでした。したがって、RHEL の将来のメジャー更新では **kernelopts** が削除され、代わりにカーネルコマンドラインパラメーターが Boot Loader Specification (BLS) スニペットに格納されます。

Bugzilla:2060759

10.9. ファイルシステムおよびストレージ

elevator カーネルコマンドラインパラメーターが非推奨になりました。

カーネルコマンドラインパラメーターの **elevator** は、すべてのデバイスのディスクスケジューラーを設定するために、以前の RHEL リリースで使用されていました。RHEL 8 では、このパラメーターが非推奨になりました。

アップストリームの Linux カーネルでは、**elevator** パラメーターに対応しなくなりましたが、互換性のために RHEL 8 でも引き続き利用できます。

カーネルは、デバイスのタイプに基づいてデフォルトのディスクスケジューラーを選択することに注意してください。これは通常、最適な設定です。別のスケジューラーが必要な場合は、**udev** ルールまたは TuneD サービスを使用して設定することが推奨されます。選択したデバイスを一致させ、それらのデバイスのスケジューラーのみを切り替えます。

詳しい情報は、ディスクスケジューラーの設定 を参照してください。

Bugzilla:1665295[1]

NFSv3 over UDP が無効になりました。

NFS サーバーは、デフォルトで UDP (User Datagram Protocol) ソケットを開いたり、リッスンしなくなりました。バージョン 4 では TCP (Transmission Control Protocol) が必要なため、この変更は NFS バージョン 3 にのみ影響を及ぼします。

RHEL 8 では、NFS over UDP に対応しなくなりました。

Bugzilla:1592011[1]

peripety が非推奨に

peripety パッケージは、RHEL 8.3 以降で非推奨になりました。

Peripety ストレージイベント通知デーモンは、システムストレージログを構造化されたストレージイベントに解析します。ストレージの問題を調査するのに役立ちます。

Bugzilla:1871953

async 以外の VDO 書き込みモードが非推奨に

VDO は、RHEL 8 で複数の書き込みモードに対応します。

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

RHEL 8.4 以降、以下の書き込みモードが非推奨になりました。

sync

VDO レイヤー上のデバイスは、VDO が同期されているかどうかを認識できないため、デバイスは VDO **sync** モードを利用できません。

async-unsafe

VDO は、ACID (Atomicity, Consistency, Isolation, and Durability) に準拠する **async** モードの回避策としてこの書き込みモードを追加しました。Red Hat は、ほとんどのユースケースで **async-unsafe** を推奨せず、それに依存するユーザーを認識しません。

auto

この書き込みモードは、他の書き込みモードのいずれかのみを選択します。VDO が 1 つの書き込みモードのみに対応している場合は、不要になりました。

この書き込みモードは、今後の RHEL メジャーリリースで削除されます。

推奨される VDO 書き込みモードが **async** になりました。

VDO 書き込みモードの詳細は、VDO 書き込みモードの選択 を参照してください。

Jira:RHELPLAN-70700[1]

VDO マネージャーが非推奨に

python ベースの VDO 管理ソフトウェアは非推奨となり、RHEL 9 から削除される予定です。RHEL 9 では、LVM-VDO 統合に置き換えられます。そのため、**lvcreate** コマンドを使用して VDO ボリュームを作成することが推奨されます。

VDO 管理ソフトウェアを使用して作成した既存のボリュームは、**lvm2** パッケージが提供する **/usr/sbin/lvm_import_vdo** スクリプトを使用して変換できます。LVM-VDO 実装の詳細は、RHEL での論理ボリュームの重複排除および圧縮 を参照してください。

Bugzilla:1949163

cramfs が非推奨になりました。

ユーザーの不足により、**cramfs** カーネルモジュールが非推奨になりました。代替策として **squashfs** が推奨されます。

Bugzilla:1794513[1]

10.10. 高可用性およびクラスター

clufter ツールに対応する pcs コマンドが非推奨になりました。

クラスター設定フォーマットを分析する **clufter** ツールに対応する **pcs** コマンドが非推奨になりました。これらのコマンドにより、コマンドが非推奨になり、コマンドに関連するセクションが **pcs** ヘルプ表示と、**pcs(8)** man ページから削除されていることを示す警告が出力されるようになりました。

以下のコマンドが非推奨になりました。

- **pcs config import-cman**: CMAN / RHEL6 HA クラスター設定のインポート
- **pcs config export**: クラスター設定を、同じクラスターを再作成する **pcs** コマンドのリストにエクスポート

Bugzilla:1851335[1]

10.11. 動的プログラミング言語、WEB サーバー、およびデータベースサーバー

Apache HTTP サーバーで使用するために PHP に提供されている mod_php モジュールが非推奨になりました。

RHEL 8 の Apache HTTP サーバーで使用するために PHP に付属している **mod_php** モジュールは利用可能ですが、デフォルト設定では有効になっていません。このモジュールは RHEL 9 では使用できなくなりました。

RHEL 8 以降、PHP スクリプトはデフォルトで FastCGI Process Manager (**php-fpm**) を使用して実行されます。詳細は、Apache HTTP サーバーでの PHP の使用 を参照してください。

Bugzilla:2225332

10.12. コンパイラーおよび開発ツール

gdb.i686 パッケージが非推奨に

RHEL 8.1 では、別のパッケージの依存関係の問題が原因で、32 ビットバージョンの GNU Debugger(GDB) **gdb.i686** が同梱されていました。RHEL 8 は 32 ビットハードウェアに対応していないため、RHEL 8.4 以降、**gdb.i686** パッケージは非推奨になりました。64 ビットバージョンの GDB (**gdb.x86_64**) は、32 ビットアプリケーションをデバッグできます。

gdb.i686 を使用する場合は、以下の重要な問題に注意してください。

- **gdb.i686** パッケージは更新されなくなりました。代わりに **gdb.x86_64** をインストールする必要があります。
- **gdb.i686** をインストールしている場合は、**gdb.x86_64** をインストールすると、**yum** が **package gdb-8.2-14.el8.x86_64 obsoletes gdb < 8.2-14.el8 provided by gdb-8.2-12.el8.i686** を報告します。これは想定される状況です。**gdb.i686** をアンインストールするか、**--allowerasing** オプションを **dnf** に渡して **gdb.i686** を削除し、**gdb.x8_64** をインストールします。
- ユーザーは、64 ビットシステム (つまり、**libc.so.6()(64-bit)** パッケージのある) に **gdb.i686** パッケージをインストールすることができなくなります。

Bugzilla:1853140[1]

libdwarf が非推奨に

RHEL 8 では、**libdwarf** ライブラリーが非推奨になりました。ライブラリーは、将来のメジャーリリースでサポートされない可能性があります。代わりに、ELF/DWARF ファイルを処理するアプリケーションに **elfutils** および **libdw** ライブラリーを使用してください。

libdwarf-tools dwarfdump プログラムの代替は、**binutils readelf** プログラムまたは **elfutils eu-readelf** プログラムになります。どちらも **--debug-dump** フラグを渡すことで使用されます。

Bugzilla:1920624

10.13. IDENTITY MANAGEMENT

openssh-ldap が非推奨に

openssh-ldap サブパッケージは、Red Hat Enterprise Linux 8 で非推奨になり、RHEL 9 で削除されます。**openssh-ldap** サブパッケージはアップストリームでは維持されないため、Red Hat は SSSD と **sss_ssh_authorizedkeys** ヘルパーを使用することを推奨しています。これは、他の IdM ソリューションよりも適切に統合でき、安全です。

デフォルトでは、**ldap** および **ipa** プロバイダーはユーザーオブジェクトの **sshPublicKey** LDAP 属性を読み取ります (利用可能な場合)。AD (Active Directory) には公開鍵を保存するためのデフォルトの LDAP 属性がないため、**ad** プロバイダーまたは IdM の信頼されるドメインのデフォルト SSSD 設定を使用して AD から SSH 公開鍵を取得することはできません。

sss_ssh_authorizedkeys ヘルパーが SSSD から鍵を取得できるようにするには、 **sssd.conf** ファイルの **services** オプションに **ssh** を追加して **ssh** レスポンダーを有効にします。詳細は man ページの **sssd.conf(5)** を参照してください。

sshd が **sss_ssh_authorizedkeys** を使用できるようにするには、man ページの **sss_ssh_authorizedkeys(1)** に記載されているように、**AuthorizedKeysCommand /usr/bin/sss_ssh_authorizedkeys** および **AuthorizedKeysCommandUser nobody** オプションを **/etc/ssh/sshd_config** ファイルに追加します。

Bugzilla:1871025

DES および 3DES 暗号化タイプが削除されました。

RHEL 7 以降、セキュリティー上の理由から、データ暗号化標準 (DES) アルゴリズムが非推奨になり、デフォルトで無効化になりました。Kerberos パッケージの最近のリベースで、RHEL 8 からシングル DES (DES) およびトリプル DES (3DES) の暗号化タイプが削除されました。

DES または 3DES の暗号化のみを使用するようにサービスまたはユーザーが設定されている場合、以下のようなサービスの中断が発生する可能性があります。

- Kerberos 認証エラー
- **unknown enctype** 暗号化エラー
- DES で暗号化されたデータベースマスターキー (**K/M**) を使用した KDC (Kerberos Distribution Center) が起動しない

アップグレードを準備するには、以下の操作を実施します。

1. KDC が **krb5check** オープンソース Python スクリプトで DES または 3DES 暗号化を使用しているかどうかを確認します。GitHub の krb5check を参照してください。
2. Kerberos プリンシパルで DES または 3DES 暗号化を使用している場合は、Advanced Encryption Standard (AES) などのサポート対象の暗号化タイプでキーを変更します。キー変更の手順については、MIT Kerberos ドキュメントの Retiring DES を参照してください。
3. アップグレードの前に以下の Kerberos オプションを一時的に設定して、DES および 3DES からの独立性をテストします。
   a. KDC の **/var/kerberos/krb5kdc/kdc.conf** で、**supported_enctypes** を設定し、**des** または **des3** は含まれません。
   b. すべてのホストについて、**/etc/krb5.conf** および **/etc/krb5.conf.d** のすべてのファイルで、**allow_weak_crypto** を **false** に設定します。デフォルトは false です。
   c. すべてのホストについて、**/etc/krb5.conf** および **/etc/krb5.conf.d** のすべてのファイルで、**permitted_enctypes**、**default_tgs_enctypes**、**default_tkt_enctypes** を設定します。また、**des** または **des3** は含めません。
4. 前の手順で Kerberos 設定をテストしてサービスが中断されない場合は、サービスを削除してアップグレードします。最新の Kerberos パッケージにアップグレードした後は、この設定は必要ありません。

Bugzilla:1877991

SSSD バージョンの libwbclient が削除される

libwbclient パッケージの SSSD 実装は、RHEL 8.4 で非推奨になりました。最新バージョンの Samba で使用できないため、 **libwbclient** の SSSD 実装 が削除されています。

Bugzilla:1947671

ctdb サービスのスタンドアロン使用が非推奨になりました。

RHEL 8.4 以降、以下の条件がすべて適用されている場合に限り、**ctdb** クラスター Samba サービスを使用することが推奨されます。

- **ctdb** サービスは、resource-agent **ctdb** を使用して **pacemaker** リソースとして管理されます。
- **ctdb** サービスは、Red Hat Gluster Storage 製品または GFS2 ファイルシステムが提供する GlusterFS ファイルシステムのいずれかが含まれるストレージボリュームを使用します。

ctdb サービスのスタンドアロンユースケースは非推奨となり、Red Hat Enterprise Linux の次期メジャーリリースには含まれません。Samba のサポートポリシーの詳細は、ナレッジベースの記事 Support Policies for RHEL Resilient Storage - ctdb General Policies を参照してください。

Bugzilla:1916296[1]

WinSync による IdM との間接的な AD 統合が非推奨に

WinSync は、さまざまな機能制限のため、RHEL 8 では積極的に開発されなくなりました。

- WinSync は、1 つの Active Directory (AD) ドメインのみをサポートします。
- パスワードの同期には、AD ドメインコントローラーに追加のソフトウェアをインストールする必要があります。

リソースとセキュリティーの分離を強化したより強固なソリューションとして、レッドハットは Active Directory との間接的な統合に**フォレスト間の信頼**を使用することを推奨しています。間接的な統合 のドキュメントを参照してください。

Jira:RHELPLAN-100400[1]

Samba を PDC または BDC として実行することは非推奨になりました。

管理者が Samba を NT4 のようなプライマリードメインコントローラー (PDC) として実行し、バックアップドメインコントローラー (BDC) を実行できるようにする従来のドメインコントローラーモードが非推奨になりました。これらのモードを設定するためのコードおよび設定は、今後の Samba リリースで削除されます。

RHEL 8 の Samba バージョンが PDC モードおよび BDC モードを提供している限り、Red Hat は、NT4 ドメインに対応する Windows バージョンを使用する既存のインストールでのみ、これらのモードをサポートします。Red Hat は、新規の Samba NT4 ドメインのセットアップを推奨しません。なぜなら、Microsoft のオペレーティングシステム (Windows 7 以降) および Windows Server 2008 R2 は、NT4 ドメインをサポートしないからです。

PDC を使用して Linux ユーザーのみを認証する場合、Red Hat は、RHEL サブスクリプションに含まれる Red Hat Identity Management (IdM) への移行を推奨します。ただし、Windows システムを IdM ドメインに参加させることはできません。Red Hat は、引き続き IdM が使用する PDC 機能のサポートを継続することに注意してください。

Red Hat は、Samba を AD ドメインコントローラー (DC) として実行することはサポートしていません。

Bugzilla:1926114

Samba で SMB1 プロトコルが非推奨になりました

Samba 4.11 以降、安全でない Server Message Block バージョン 1 (SMB1) プロトコルは非推奨となり、今後のリリースでは削除される予定です。

セキュリティーを向上させるために、デフォルトでは、Samba サーバーおよびクライアントユーティリティーで SMB1 が無効になっています。

Jira:RHELDOCS-16612[1]

FreeRADIUS のサポートは限定的です

RHEL 8 では、FreeRADIUS サービスの一部として、次の外部認証モジュールが非推奨になりました。

- MySQL、PostgreSQL、SQlite、および unixODBC データベースコネクター
- **Perl** 言語モジュール
- REST API モジュール

注記

ベースパッケージの一部として提供される PAM 認証モジュールおよびその他の認証モジュールは影響を受けません。

廃止されたモジュールの代替は、Fedora プロジェクトなどのコミュニティーでサポートされているパッケージで見つけることができます。

さらに、**freeradius** パッケージのサポート範囲は、将来の RHEL リリースでは次のユースケースに限定されます。

- FreeRADIUS をワイヤレス認証プロバイダーとして使用し、Identity Management (IdM) を認証のバックエンドソースとして使用します。認証は、**krb5** および LDAP 認証パッケージを使用して、またはメインの FreeRADIUS パッケージの PAM 認証として行われます。
- FreeRADIUS を使用して、Python 3 認証パッケージで IdM の認証用に信頼できる情報源を提供します。

これらの廃止とは対照的に、Red Hat は FreeRADIUS による次の外部認証モジュールのサポートを強化します。

- **krb5** および LDAP に基づく認証
- **Python 3** 認証

これらのインテグレーションオプションに重点を置くことは、Red Hat IdM の戦略的方向性に一致します。

Jira:RHELDOCS-17573

10.14. デスクトップ

libgnome-keyring ライブラリーが非推奨になりました。

libgnome-keyring ライブラリーがアップストリームで維持されず、RHEL に必要な暗号化ポリシーに従っていないため、**libsecret** ライブラリーが **libgnome-keyring** ライブラリーを引き継ぎ、libgnome-keyring は非推奨となりました。新しい **libsecret** ライブラリーは、必要なセキュリティー標準に準拠する代替ライブラリーです。

Bugzilla:1607766[1]

LibreOffice が非推奨になりました

LibreOffice RPM パッケージは非推奨となり、今後の RHEL メジャーリリースで削除される予定です。LibreOffice は、RHEL 7、8、および 9 のライフサイクル全体を通じて引き続き完全にサポートされます。

Red Hat は、RPM パッケージの代わりに、The Document Foundation が提供する次のいずれかのソースから LibreOffice をインストールすることを推奨します。

- Flathub リポジトリーの公式 Flatpak パッケージ: https://flathub.org/apps/org.libreoffice.LibreOffice
- 公式 RPM パッケージ: https://www.libreoffice.org/download/download-libreoffice/

Jira:RHELDOCS-16300[1]

10.15. グラフィックインフラストラクチャー

AGP グラフィックカードがサポートされなくなりました。

AGP (Accelerated Graphics Port) バスを使用するグラフィックカードは、Red Hat Enterprise Linux 8 ではサポートされていません。推奨される代替として、PCI-Express バスを備えたグラフィックスカードを使用してください。

Bugzilla:1569610[1]

Motif が非推奨になりました

アップストリームの Motif コミュニティーでの開発は非アクティブであるため、Motif ウィジェットツールキットは RHEL で非推奨になりました。

開発バリアントおよびデバッグバリアントを含む、以下の Motif パッケージが非推奨になりました。

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

さらに、**motif-static** パッケージが削除されました。

Red Hat は、GTK ツールキットを代替として使用することを推奨します。GTK は Motif と比較してメンテナンス性が高く、新機能を提供します。

Jira:RHELPLAN-98983[1]

10.16. WEB コンソール

Web コンソールは、不完全な翻訳への対応を終了しました。

RHEL Web コンソールは、コンソールの翻訳可能な文字列の翻訳率が 50 % 未満の言語に対する翻訳提供を廃止しました。ブラウザーがこのような言語に翻訳を要求すると、ユーザーインターフェイスは英語になります。

Bugzilla:1666722

remotectl コマンドは非推奨になりました

remotectl コマンドは非推奨となり、RHEL の将来のリリースでは使用できなくなります。代わりに **cockpit-certificate-ensure** コマンドを使用できます。ただし、**cockpit-certificate-ensure** には **remotectl** と同等の機能がないことに注意してください。バンドルされた証明書とキーチェーンファイルはサポートされていないため、それらを分割する必要があります。

Jira:RHELPLAN-147538[1]

10.17. RED HAT ENTERPRISE LINUX システムロール

geoipupdate パッケージが非推奨に

geoipupdate パッケージにはサードパーティーのサブスクリプションが必要で、プロプライエタリーコンテンツもダウンロードします。したがって、**geoipupdate** パッケージは非推奨となり、次の RHEL メジャーバージョンで削除されます。

Bugzilla:1874892[1]

RHEL 9 ノードでチームを設定すると、 network システムロールが非推奨の警告を表示します

ネットワークチーミング機能は、RHEL 9 では非推奨になりました。その結果、RHEL 8 制御ノードで **ネットワーク** RHEL システムロールを使用して RHEL 9 ノードでネットワークチームを設定すると、非推奨に関する警告が表示されます。

Bugzilla:2021685

Ansible Engine は非推奨になりました

以前のバージョンの RHEL 8 では、RHEL システムロールや Insights 修復などのサポートされている RHEL Automation ユースケースを有効にするために、サポート範囲が限定された Ansible Engine リポジトリーへのアクセスが提供されていました。Ansible Engine は非推奨になり、Ansible Engine 2.9 は 2023 年 9 月 29 日以降サポートされなくなります。サポートされているユースケースの詳細については、RHEL 9 および RHEL 8.6 以降の AppStream リポジトリーに含まれる Ansible Core パッケージのサポート対象範囲 を参照してください。

ユーザーは、システムを Ansible Engine から Ansible Core に手動で移行する必要があります。そのためには、以下の手順に従います。

手順

1. システムが RHEL 8.7 以降のリリースを実行しているかどうかを確認します。

```
# cat /etc/redhat-release
```

2. Ansible Engine 2.9 をインストールします。

```
# yum remove ansible
```

3. **ansible-2-for-rhel-8-x86_64-rpms** リポジトリーを無効にします。

```
# subscription-manager repos --disable
ansible-2-for-rhel-8-x86_64-rpms
```

4. RHEL 8 AppStream リポジトリーから Ansible Core パッケージをインストールします。

```
# yum install ansible-core
```

詳細については、RHEL8.6 以降での Ansible の使用 を参照してください。

Bugzilla:2006081

10.18. 仮想化

virsh iface-* コマンドが非推奨になりました。

virsh iface-start、**virsh iface-destroy** などの **virsh iface-*** コマンドは非推奨になり、将来のメジャーバージョンの RHEL では削除される予定です。また、このようなコマンドは設定の依存関係により頻繁に失敗します。

したがって、ホストネットワーク接続の設定および管理には **virsh iface-*** コマンドを使用しないことが推奨されます。代わりに、NetworkManager プログラムと、関連する管理アプリケーション (**nmcli** など) を使用します。

Bugzilla:1664592[1]

virt-manager が非推奨になりました

Virtual Machine Manager アプリケーション (**virt-manager**) は非推奨になっています。RHEL Web コンソール (**Cockpit**) は、後続のリリースで置き換えられる予定です。したがって、GUI で仮想化を管理する場合は、Web コンソールを使用することが推奨されます。ただし、**virt-manager** で利用可能な機能によっては、RHEL Web コンソールで利用できない場合があります。

Jira:RHELPLAN-10304[1]

仮想マシンスナップショットのサポートが限定されました

仮想マシンのスナップショットの作成は、現在、UEFI ファームウェアを使用していない仮想マシンのみでサポートされています。さらに、スナップショット操作中に QEMU モニターがブロックされる可能性があり、これは特定のワークロードのハイパーバイザーのパフォーマンスに悪影響を及ぼします。

また、現在の仮想マシンスナップショットの作成メカニズムは非推奨となり、Red Hat は実稼働環境での仮想マシンスナップショットの使用を推奨していないことにも注意してください。

Bugzilla:1686057

Cirrus VGA 仮想 GPU タイプが非推奨に

Red Hat Enterprise Linux の今後のメジャー更新では、KVM 仮想マシンで **Cirrus VGA** GPU デバイスに対応しなくなります。したがって、Red Hat は **Cirrus VGA** の代わりに **stdvga** または **virtio-vga** デバイスの使用を推奨します。

Bugzilla:1651994[1]

SPICE が非推奨になりました

SPICE リモートディスプレイプロトコルが非推奨になりました。その結果、SPICE は RHEL 8 で引き続きサポートされますが、Red Hat では、リモートディスプレイストリーミングに代替ソリューションを使用することを推奨しています。

- リモートコンソールへのアクセスには、VNC プロトコルを使用します。
- 高度なリモートディスプレイ機能には、RDP、HP RGS、または Mechdyne TGX などのサードパーティーツールを使用します。

SPICE で使用される **QXL** グラフィックスデバイスも非推奨になっていることに注意してください。

Bugzilla:1849563[1]

IBM POWER 上の KVM が非推奨に

IBM POWER ハードウェアでの KVM 仮想化の使用は非推奨になりました。その結果、IBM POWER の KVM は、RHEL 8 でも引き続きサポートされますが、RHEL の今後のメジャーリリースではサポートされなくなります。

Jira:RHELPLAN-71200[1]

SHA1 ベースの署名を使用した SecureBoot イメージ検証が非推奨になりました

UEFI (PE/COFF) 実行ファイルでの SHA1 ベースの署名を使用した SecureBoot イメージ検証の実行は非推奨になりました。代わりに、Red Hat は、SHA2 アルゴリズムまたはそれ以降に基づく署名を使用することを推奨します。

Bugzilla:1935497[1]

SPICE を使用したスマートカードリーダーの仮想マシンへの接続が非推奨となりました

RHEL 8 では、SPICE リモートディスプレイプロトコルが非推奨になりました。スマートカードリーダーを仮想マシンに割り当てる唯一の推奨される方法は、SPICE プロトコルに依存するため、仮想マシンでのスマートカードの使用も RHEL 8 で非推奨になりました。

RHEL の将来のメジャーバージョンでは、スマートカードリーダーを仮想マシンに割り当てる機能は、サードパーティーのリモート可視化ソリューションでのみサポートされる予定です。

Bugzilla:2059626

RDMA ベースのライブマイグレーションは非推奨になりました。

この更新により、リモートダイレクトメモリーアクセス (RDMA) を使用した実行中の仮想マシンの移行は非推奨になりました。その結果、**rdma:**// 移行 URI を使用して RDMA 経由の移行を要求することは可能ですが、この機能は RHEL の将来のメジャーリリースではサポートされなくなります。

Jira:RHELPLAN-153267[1]

10.19. コンテナー

Podman varlink ベースの API v1.0 が削除されました

Podman varlink ベースの API v1.0 は、以前のリリースの RHEL 8 で非推奨となりました。Podman v2.0 には、新しい Podman v2.0 RESTful API が導入されました。Podman v3.0 のリリースでは、varlink ベースの API v1.0 が完全に削除されました。

Jira:RHELPLAN-45858[1]

container-tools:1.0 が非推奨に

container-tools:1.0 モジュールは非推奨となり、セキュリティー更新を受信しなくなります。**container-tools:2.0** や **container-tools:3.0** などの新しいサポートされる安定したモジュールストリームを使用することが推奨されます。

Jira:RHELPLAN-59825[1]

container-tools:2.0 モジュールは非推奨になりました

container-tools:2.0 モジュールは非推奨となり、セキュリティー更新を受信しなくなります。**container-tools:3.0** など、サポートされている新しい安定したモジュールストリームの使用を推奨します。

Jira:RHELPLAN-85066[1]

GIMP 以外の Flatpak イメージは廃止されました

rhel8/firefox-flatpak、**rhel8/thunderbird-flatpak**、**rhel8/inkscape-flatpak**、および **rhel8/libreoffice-flatpak** RHEL 8 Flatpak アプリケーションは廃止され、RHEL 9 バージョンに置き換えられました。RHEL 9 にはまだ代替品がないため、**rhel8/gimp-flatpak** Flatpak アプリケーションは非推奨ではありません。

Bugzilla:2142499

CNI ネットワークスタックが非推奨になりました

Container Network Interface (CNI) ネットワークスタックは非推奨となり、RHEL の今後のマイナーリリースでは Podman から削除される予定です。以前は、コンテナーは DNS 経由のみで単一の Container Network Interface (CNI) プラグインに接続していました。Podman v.4.0 では、新しい Netavark ネットワークスタックが導入されました。Netavark ネットワークスタックは、Podman およびその他の Open Container Initiative (OCI) コンテナー管理アプリケーションとともに使用できます。Podman 用の Netavark ネットワークスタックは、高度な Docker 機能とも互換性があります。複数のネットワーク内のコンテナーは、それらのネットワークのいずれかにあるコンテナーにアクセスできます。

詳細は、CNI から Netavark へのネットワークスタックの切り替え を参照してください。

Jira:RHELDOCS-16755[1]

container-tools:3.0 が非推奨になりました。

container-tools:3.0 モジュールは非推奨となり、セキュリティー更新を受信しなくなります。RHEL 上で Linux コンテナーの構築と実行を続けるには、**container-tools:4.0** など、より新しく安定したサポートされているモジュールストリームを使用してください。

後続のストリームに切り替える手順については、後続のストリームへの切り替え を参照してください。

Jira:RHELPLAN-146398[1]

Inkscape および LibreOffice Flatpak イメージが非推奨になりました

テクノロジープレビューとして利用可能な **rhel9/inkscape-flatpak** および **rhel9/libreoffice-flatpak** Flatpak イメージは非推奨になりました。

Red Hat は、これらのイメージに代わる次の代替手段を推奨します。

- **rhel9/inkscape-flatpak** を置き換えるには、**inkscape** RPM パッケージを使用します。

- **rhel9/libreoffice-flatpak** を置き換えるには、LibreOffice 非推奨化に関するリリースノート を参照してください。

Jira:RHELDOCS-17102[1]

10.20. 非推奨のパッケージ

このセクションでは、非推奨となり、将来バージョンの Red Hat Enterprise Linux には含まれない可能性があるパッケージのリストを示します。

RHEL 7 と RHEL 8 との間でパッケージを変更する場合は、**RHEL 8 の導入における考慮事項** ドキュメントの パッケージの変更 を参照してください。

重要

非推奨パッケージのサポート状況は、RHEL 8 内でも変更されません。サポート期間の詳細は、Red Hat Enterprise Linux のライフサイクル および Red Hat Enterprise Linux アプリケーションストリームのライフサイクル を参照してください。

次のパッケージは RHEL 8 で非推奨になりました。

- 389-ds-base-legacy-tools
- abrt
- abrt-addon-ccpp
- abrt-addon-kerneloops
- abrt-addon-pstoreoops
- abrt-addon-vmcore
- abrt-addon-xorg
- abrt-cli
- abrt-console-notification
- abrt-dbus
- abrt-desktop
- abrt-gui
- abrt-gui-libs
- abrt-libs
- abrt-tui
- adobe-source-sans-pro-fonts
- adwaita-qt
- alsa-plugins-pulseaudio

- amanda
- amanda-client
- amanda-libs
- amanda-server
- ant-contrib
- antlr3
- antlr32
- aopalliance
- apache-commons-collections
- apache-commons-compress
- apache-commons-exec
- apache-commons-jxpath
- apache-commons-parent
- apache-ivy
- apache-parent
- apache-resource-bundles
- apache-sshd
- apiguardian
- aspnetcore-runtime-3.0
- aspnetcore-runtime-3.1
- aspnetcore-runtime-5.0
- aspnetcore-targeting-pack-3.0
- aspnetcore-targeting-pack-3.1
- aspnetcore-targeting-pack-5.0
- assertj-core
- authd
- auto
- autoconf213
- autogen

- autogen-libopts
- awscli
- base64coder
- batik
- batik-css
- batik-util
- bea-stax
- bea-stax-api
- bind-export-devel
- bind-export-libs
- bind-libs-lite
- bind-pkcs11
- bind-pkcs11-devel
- bind-pkcs11-libs
- bind-pkcs11-utils
- bind-sdb
- bind-sdb
- bind-sdb-chroot
- bluez-hid2hci
- boost-jam
- boost-signals
- bouncycastle
- bpg-algeti-fonts
- bpg-chveulebrivi-fonts
- bpg-classic-fonts
- bpg-courier-fonts
- bpg-courier-s-fonts
- bpg-dedaena-block-fonts
- bpg-dejavu-sans-fonts

- bpg-elite-fonts
- bpg-excelsior-caps-fonts
- bpg-excelsior-condenced-fonts
- bpg-excelsior-fonts
- bpg-fonts-common
- bpg-glaho-fonts
- bpg-gorda-fonts
- bpg-ingiri-fonts
- bpg-irubaqidze-fonts
- bpg-mikhail-stephan-fonts
- bpg-mrgvlovani-caps-fonts
- bpg-mrgvlovani-fonts
- bpg-nateli-caps-fonts
- bpg-nateli-condenced-fonts
- bpg-nateli-fonts
- bpg-nino-medium-cond-fonts
- bpg-nino-medium-fonts
- bpg-sans-fonts
- bpg-sans-medium-fonts
- bpg-sans-modern-fonts
- bpg-sans-regular-fonts
- bpg-serif-fonts
- bpg-serif-modern-fonts
- bpg-ucnobi-fonts
- brlapi-java
- bsh
- buildnumber-maven-plugin
- byaccj
- cal10n

- cbi-plugins
- cdparanoia
- cdparanoia-devel
- cdparanoia-libs
- cdrdao
- cmirror
- codehaus-parent
- codemodel
- compat-exiv2-026
- compat-guile18
- compat-hwloc1
- compat-libpthread-nonshared
- compat-libtiff3
- compat-openssl10
- compat-sap-c++-11
- compat-sap-c++-10
- compat-sap-c++-9
- createrepo_c-devel
- ctags
- ctags-etags
- custodia
- cyrus-imapd-vzic
- dbus-c++
- dbus-c++-devel
- dbus-c++-glib
- dbxtool
- dhcp-libs
- directory-maven-plugin
- directory-maven-plugin-javadoc

- dirsplit
- dleyna-connector-dbus
- dleyna-core
- dleyna-renderer
- dleyna-server
- dnssec-trigger
- dnssec-trigger-panel
- dotnet-apphost-pack-3.0
- dotnet-apphost-pack-3.1
- dotnet-apphost-pack-5.0
- dotnet-host-fxr-2.1
- dotnet-host-fxr-2.1
- dotnet-hostfxr-3.0
- dotnet-hostfxr-3.1
- dotnet-hostfxr-5.0
- dotnet-runtime-2.1
- dotnet-runtime-3.0
- dotnet-runtime-3.1
- dotnet-runtime-5.0
- dotnet-sdk-2.1
- dotnet-sdk-2.1.5xx
- dotnet-sdk-3.0
- dotnet-sdk-3.1
- dotnet-sdk-5.0
- dotnet-targeting-pack-3.0
- dotnet-targeting-pack-3.1
- dotnet-targeting-pack-5.0
- dotnet-templates-3.0
- dotnet-templates-3.1

- dotnet-templates-5.0
- dotnet5.0-build-reference-packages
- dptfxtract
- drpm
- drpm-devel
- dump
- dvd+rw-tools
- dyninst-static
- eclipse-ecf
- eclipse-ecf-core
- eclipse-ecf-runtime
- eclipse-emf
- eclipse-emf-core
- eclipse-emf-runtime
- eclipse-emf-xsd
- eclipse-equinox-osgi
- eclipse-jdt
- eclipse-license
- eclipse-p2-discovery
- eclipse-pde
- eclipse-platform
- eclipse-swt
- ed25519-java
- ee4j-parent
- elfutils-devel-static
- elfutils-libelf-devel-static
- enca
- enca-devel
- environment-modules-compat

- evince-browser-plugin
- exec-maven-plugin
- farstream02
- felix-gogo-command
- felix-gogo-runtime
- felix-gogo-shell
- felix-scr
- felix-osgi-compendium
- felix-osgi-core
- felix-osgi-foundation
- felix-parent
- file-roller
- fipscheck
- fipscheck-devel
- fipscheck-lib
- firewire
- fonts-tweak-tool
- forge-parent
- freeradius-mysql
- freeradius-perl
- freeradius-postgresql
- freeradius-rest
- freeradius-sqlite
- freeradius-unixODBC
- fuse-sshfs
- fusesource-pom
- future
- gamin
- gamin-devel

- gavl
- gcc-toolset-9
- gcc-toolset-9-annobin
- gcc-toolset-9-build
- gcc-toolset-9-perftools
- gcc-toolset-9-runtime
- gcc-toolset-9-toolchain
- gcc-toolset-10
- gcc-toolset-10-annobin
- gcc-toolset-10-binutils
- gcc-toolset-10-binutils-devel
- gcc-toolset-10-build
- gcc-toolset-10-dwz
- gcc-toolset-10-dyninst
- gcc-toolset-10-dyninst-devel
- gcc-toolset-10-elfutils
- gcc-toolset-10-elfutils-debuginfod-client
- gcc-toolset-10-elfutils-debuginfod-client-devel
- gcc-toolset-10-elfutils-devel
- gcc-toolset-10-elfutils-libelf
- gcc-toolset-10-elfutils-libelf-devel
- gcc-toolset-10-elfutils-libs
- gcc-toolset-10-gcc
- gcc-toolset-10-gcc-c++
- gcc-toolset-10-gcc-gdb-plugin
- gcc-toolset-10-gcc-gfortran
- gcc-toolset-10-gdb
- gcc-toolset-10-gdb-doc
- gcc-toolset-10-gdb-gdbserver

- gcc-toolset-10-libasan-devel
- gcc-toolset-10-libatomic-devel
- gcc-toolset-10-libitm-devel
- gcc-toolset-10-liblsan-devel
- gcc-toolset-10-libquadmath-devel
- gcc-toolset-10-libstdc++-devel
- gcc-toolset-10-libstdc++-docs
- gcc-toolset-10-libtsan-devel
- gcc-toolset-10-libubsan-devel
- gcc-toolset-10-ltrace
- gcc-toolset-10-make
- gcc-toolset-10-make-devel
- gcc-toolset-10-perftools
- gcc-toolset-10-runtime
- gcc-toolset-10-strace
- gcc-toolset-10-systemtap
- gcc-toolset-10-systemtap-client
- gcc-toolset-10-systemtap-devel
- gcc-toolset-10-systemtap-initscript
- gcc-toolset-10-systemtap-runtime
- gcc-toolset-10-systemtap-sdt-devel
- gcc-toolset-10-systemtap-server
- gcc-toolset-10-toolchain
- gcc-toolset-10-valgrind
- gcc-toolset-10-valgrind-devel
- gcc-toolset-11-make-devel
- GConf2
- GConf2-devel
- gegl

- genisoimage
- genwqe-tools
- genwqe-vpd
- genwqe-zlib
- genwqe-zlib-devel
- geoipupdate
- geronimo-annotation
- geronimo-jms
- geronimo-jpa
- geronimo-parent-poms
- gfbgraph
- gflags
- gflags-devel
- glassfish-annotation-api
- glassfish-el
- glassfish-fastinfoset
- glassfish-jaxb-core
- glassfish-jaxb-txw2
- glassfish-jsp
- glassfish-jsp-api
- glassfish-legal
- glassfish-master-pom
- glassfish-servlet-api
- glew-devel
- glib2-fam
- glog
- glog-devel
- gmock
- gmock-devel

- gnome-abrt
- gnome-boxes
- gnome-menus-devel
- gnome-online-miners
- gnome-shell-extension-disable-screenshield
- gnome-shell-extension-horizontal-workspaces
- gnome-shell-extension-no-hot-corner
- gnome-shell-extension-window-grouper
- gnome-themes-standard
- gnu-free-fonts-common
- gnu-free-mono-fonts
- gnu-free-sans-fonts
- gnu-free-serif-fonts
- gnupg2-smime
- gnuplot
- gnuplot-common
- gobject-introspection-devel
- google-gson
- google-noto-sans-syriac-eastern-fonts
- google-noto-sans-syriac-estrangela-fonts
- google-noto-sans-syriac-western-fonts
- google-noto-sans-tibetan-fonts
- google-noto-sans-ui-fonts
- gphoto2
- gsl-devel
- gssntlmssp
- gtest
- gtest-devel
- gtkmm24

- gtkmm24-devel
- gtkmm24-docs
- gtksourceview3
- gtksourceview3-devel
- gtkspell
- gtkspell-devel
- gtkspell3
- guile
- gutenprint-gimp
- gutenprint-libs-ui
- gvfs-afc
- gvfs-afp
- gvfs-archive
- hamcrest-core
- hawtjni
- hawtjni
- hawtjni-runtime
- HdrHistogram
- HdrHistogram-javadoc
- highlight-gui
- hivex-devel
- hostname
- hplip-gui
- httpcomponents-project
- hwloc-plugins
- hyphen-fo
- hyphen-grc
- hyphen-hsb
- hyphen-ia

- hyphen-is
- hyphen-ku
- hyphen-mi
- hyphen-mn
- hyphen-sa
- hyphen-tk
- ibus-sayura
- icedax
- icu4j
- idm-console-framework
- inkscape
- inkscape-docs
- inkscape-view
- iptables
- ipython
- isl
- isl-devel
- isorelax
- istack-commons-runtime
- istack-commons-tools
- iwl3945-firmware
- iwl4965-firmware
- iwl6000-firmware
- jacoco
- jaf
- jaf-javadoc
- jakarta-oro
- janino
- jansi-native

- jarjar
- java-1.8.0-ibm
- java-1.8.0-ibm-demo
- java-1.8.0-ibm-devel
- java-1.8.0-ibm-headless
- java-1.8.0-ibm-jdbc
- java-1.8.0-ibm-plugin
- java-1.8.0-ibm-src
- java-1.8.0-ibm-webstart
- java-1.8.0-openjdk-accessibility
- java-1.8.0-openjdk-accessibility-slowdebug
- java_cup
- java-atk-wrapper
- javacc
- javacc-maven-plugin
- javaewah
- javaparser
- javapoet
- javassist
- javassist-javadoc
- jaxen
- jboss-annotations-1.2-api
- jboss-interceptors-1.2-api
- jboss-logmanager
- jboss-parent
- jctools
- jdepend
- jdependency
- jdom

- jdom2
- jetty
- jetty-continuation
- jetty-http
- jetty-io
- jetty-security
- jetty-server
- jetty-servlet
- jetty-util
- jffi
- jflex
- jgit
- jline
- jmc
- jnr-netdb
- jolokia-jvm-agent
- js-uglify
- jsch
- json_simple
- jss-javadoc
- jtidy
- junit5
- jvnet-parent
- jzlib
- kernel-cross-headers
- ksc
- kurdit-unikurd-web-fonts
- kyotocabinet-libs
- ldapjdk-javadoc

- lensfun
- lensfun-devel
- lftp-scripts
- libaec
- libaec-devel
- libappindicator-gtk3
- libappindicator-gtk3-devel
- libatomic-static
- libavc1394
- libblocksruntime
- libcacard
- libcacard-devel
- libcgroup
- libcgroup-tools
- libchamplain
- libchamplain-devel
- libchamplain-gtk
- libcroco
- libcroco-devel
- libcxl
- libcxl-devel
- libdap
- libdap-devel
- libdazzle-devel
- libdbusmenu
- libdbusmenu-devel
- libdbusmenu-doc
- libdbusmenu-gtk3
- libdbusmenu-gtk3-devel

- libdc1394
- libdnet
- libdnet-devel
- libdv
- libdwarf
- libdwarf-devel
- libdwarf-static
- libdwarf-tools
- libeasyfc
- libeasyfc-gobject
- libepubgen-devel
- libertas-sd8686-firmware
- libertas-usb8388-firmware
- libertas-usb8388-olpc-firmware
- libgdither
- libGLEW
- libgovirt
- libguestfs-benchmarking
- libguestfs-devel
- libguestfs-gfs2
- libguestfs-gobject
- libguestfs-gobject-devel
- libguestfs-java
- libguestfs-java-devel
- libguestfs-javadoc
- libguestfs-man-pages-ja
- libguestfs-man-pages-uk
- libguestfs-tools
- libguestfs-tools-c

- libhugetlbfs
- libhugetlbfs-devel
- libhugetlbfs-utils
- libIDL
- libIDL-devel
- libidn
- libiec61883
- libindicator-gtk3
- libindicator-gtk3-devel
- libiscsi-devel
- libjose-devel
- libkkc
- libkkc-common
- libkkc-data
- libldb-devel
- liblogging
- libluksmeta-devel
- libmalaga
- libmcpp
- libmemcached
- libmemcached-libs
- libmetalink
- libmodulemd1
- libmongocrypt
- libmtp-devel
- libmusicbrainz5
- libmusicbrainz5-devel
- libnbd-devel
- liboauth

- liboauth-devel
- libpfm-static
- libpng12
- libpurple
- libpurple-devel
- libraw1394
- libreport-plugin-mailx
- libreport-plugin-rhtsupport
- libreport-plugin-ureport
- libreport-rhel
- libreport-rhel-bugzilla
- librpmem
- librpmem-debug
- librpmem-devel
- libsass
- libsass-devel
- libselinux-python
- libsqlite3x
- libtalloc-devel
- libtar
- libtdb-devel
- libtevent-devel
- libtpms-devel
- libunwind
- libusal
- libvarlink
- libverto-libevent
- libvirt-admin
- libvirt-bash-completion

- libvirt-daemon-driver-storage-gluster
- libvirt-daemon-driver-storage-iscsi-direct
- libvirt-devel
- libvirt-docs
- libvirt-gconfig
- libvirt-gobject
- libvirt-lock-sanlock
- libvirt-wireshark
- libvmem
- libvmem-debug
- libvmem-devel
- libvmmalloc
- libvmmalloc-debug
- libvmmalloc-devel
- libvncserver
- libwinpr-devel
- libwmf
- libwmf-devel
- libwmf-lite
- libXNVCtrl
- libyami
- log4j12
- log4j12-javadoc
- lohit-malayalam-fonts
- lohit-nepali-fonts
- lorax-composer
- lua-guestfs
- lucene
- lucene-analysis

- lucene-analyzers-smartcn
- lucene-queries
- lucene-queryparser
- lucene-sandbox
- lz4-java
- lz4-java-javadoc
- mailman
- mailx
- make-devel
- malaga
- malaga-suomi-voikko
- marisa
- maven-antrun-plugin
- maven-assembly-plugin
- maven-clean-plugin
- maven-dependency-analyzer
- maven-dependency-plugin
- maven-doxia
- maven-doxia-sitetools
- maven-install-plugin
- maven-invoker
- maven-invoker-plugin
- maven-parent
- maven-plugins-pom
- maven-reporting-api
- maven-reporting-impl
- maven-resolver-api
- maven-resolver-connector-basic
- maven-resolver-impl

- maven-resolver-spi
- maven-resolver-transport-wagon
- maven-resolver-util
- maven-scm
- maven-script-interpreter
- maven-shade-plugin
- maven-shared
- maven-verifier
- maven-wagon-file
- maven-wagon-http
- maven-wagon-http-shared
- maven-wagon-provider-api
- maven2
- meanwhile
- mercurial
- mercurial-hgk
- metis
- metis-devel
- mingw32-bzip2
- mingw32-bzip2-static
- mingw32-cairo
- mingw32-expat
- mingw32-fontconfig
- mingw32-freetype
- mingw32-freetype-static
- mingw32-gstreamer1
- mingw32-harfbuzz
- mingw32-harfbuzz-static
- mingw32-icu

- mingw32-libjpeg-turbo
- mingw32-libjpeg-turbo-static
- mingw32-libpng
- mingw32-libpng-static
- mingw32-libtiff
- mingw32-libtiff-static
- mingw32-openssl
- mingw32-readline
- mingw32-sqlite
- mingw32-sqlite-static
- mingw64-adwaita-icon-theme
- mingw64-bzip2
- mingw64-bzip2-static
- mingw64-cairo
- mingw64-expat
- mingw64-fontconfig
- mingw64-freetype
- mingw64-freetype-static
- mingw64-gstreamer1
- mingw64-harfbuzz
- mingw64-harfbuzz-static
- mingw64-icu
- mingw64-libjpeg-turbo
- mingw64-libjpeg-turbo-static
- mingw64-libpng
- mingw64-libpng-static
- mingw64-libtiff
- mingw64-libtiff-static
- mingw64-nettle

- mingw64-openssl
- mingw64-readline
- mingw64-sqlite
- mingw64-sqlite-static
- modello
- mojo-parent
- mongo-c-driver
- mousetweaks
- mozjs52
- mozjs52-devel
- mozjs60
- mozjs60-devel
- mozvoikko
- msv-javadoc
- msv-manual
- munge-maven-plugin
- mythes-mi
- mythes-ne
- nafees-web-naskh-fonts
- nbd
- nbdkit-devel
- nbdkit-example-plugins
- nbdkit-gzip-plugin
- nbdkit-plugin-python-common
- nbdkit-plugin-vddk
- ncompress
- ncurses-compat-libs
- net-tools
- netcf

- netcf-devel
- netcf-libs
- network-scripts
- network-scripts-ppp
- nkf
- nodejs-devel
- nodejs-packaging
- nss_nis
- nss-pam-ldapd
- objectweb-asm
- objectweb-asm-javadoc
- objectweb-pom
- ocaml-bisect-ppx
- ocaml-camlp4
- ocaml-camlp4-devel
- ocaml-lwt
- ocaml-mmap
- ocaml-ocplib-endian
- ocaml-ounit
- ocaml-result
- ocaml-seq
- opencryptoki-tpmtok
- opencv-contrib
- opencv-core
- opencv-devel
- openhpi
- openhpi-libs
- OpenIPMI-perl
- openssh-cavs

- openssh-ldap
- openssl-ibmpkcs11
- opentest4j
- os-maven-plugin
- pakchois
- pandoc
- paps-libs
- paranamer
- parfait
- parfait-examples
- parfait-javadoc
- pcp-parfait-agent
- pcp-pmda-rpm
- pcp-pmda-vmware
- pcsc-lite-doc
- peripety
- perl-B-Debug
- perl-B-Lint
- perl-Class-Factory-Util
- perl-Class-ISA
- perl-DateTime-Format-HTTP
- perl-DateTime-Format-Mail
- perl-File-CheckTree
- perl-homedir
- perl-libxml-perl
- perl-Locale-Codes
- perl-Mozilla-LDAP
- perl-NKF
- perl-Object-HashBase-tools

- perl-Package-DeprecationManager
- perl-Pod-LaTeX
- perl-Pod-Plainer
- perl-prefork
- perl-String-CRC32
- perl-SUPER
- perl-Sys-Virt
- perl-tests
- perl-YAML-Syck
- phodav
- php-recode
- php-xmlrpc
- pidgin
- pidgin-devel
- pidgin-sipe
- pinentry-emacs
- pinentry-gtk
- pipewire0.2-devel
- pipewire0.2-libs
- platform-python-coverage
- plexus-ant-factory
- plexus-bsh-factory
- plexus-cli
- plexus-component-api
- plexus-component-factories-pom
- plexus-components-pom
- plexus-i18n
- plexus-interactivity
- plexus-pom

- plexus-velocity
- plymouth-plugin-throbgress
- pmreorder
- postgresql-test-rpm-macros
- powermock
- prometheus-jmx-exporter
- prometheus-jmx-exporter-openjdk11
- ptscotch-mpich
- ptscotch-mpich-devel
- ptscotch-mpich-devel-parmetis
- ptscotch-openmpi
- ptscotch-openmpi-devel
- purple-sipe
- pygobject2-doc
- pygtk2
- pygtk2-codegen
- pygtk2-devel
- pygtk2-doc
- python-nose-docs
- python-nss-doc
- python-podman-api
- python-psycopg2-doc
- python-pymongo-doc
- python-redis
- python-schedutils
- python-slip
- python-sqlalchemy-doc
- python-varlink
- python-virtualenv-doc

- python2-backports
- python2-backports-ssl_match_hostname
- python2-bson
- python2-coverage
- python2-docs
- python2-docs-info
- python2-funcsigs
- python2-ipaddress
- python2-mock
- python2-nose
- python2-numpy-doc
- python2-psycopg2-debug
- python2-psycopg2-tests
- python2-pymongo
- python2-pymongo-gridfs
- python2-pytest-mock
- python2-sqlalchemy
- python2-tools
- python2-virtualenv
- python3-bson
- python3-click
- python3-coverage
- python3-cpio
- python3-custodia
- python3-docs
- python3-flask
- python3-gevent
- python3-gobject-base
- python3-hivex

- python3-html5lib
- python3-hypothesis
- python3-ipatests
- python3-itsdangerous
- python3-jwt
- python3-libguestfs
- python3-mock
- python3-networkx-core
- python3-nose
- python3-nss
- python3-openipmi
- python3-pillow
- python3-ptyprocess
- python3-pydbus
- python3-pymongo
- python3-pymongo-gridfs
- python3-pyOpenSSL
- python3-pytoml
- python3-reportlab
- python3-schedutils
- python3-scons
- python3-semantic_version
- python3-slip
- python3-slip-dbus
- python3-sqlalchemy
- python3-syspurpose
- python3-virtualenv
- python3-webencodings
- python3-werkzeug

- python38-asn1crypto
- python38-numpy-doc
- python38-psycopg2-doc
- python38-psycopg2-tests
- python39-numpy-doc
- python39-psycopg2-doc
- python39-psycopg2-tests
- qemu-kvm-block-gluster
- qemu-kvm-block-iscsi
- qemu-kvm-block-ssh
- qemu-kvm-hw-usbredir
- qemu-kvm-device-display-virtio-gpu-gl
- qemu-kvm-device-display-virtio-gpu-pci-gl
- qemu-kvm-device-display-virtio-vga-gl
- qemu-kvm-tests
- qpdf
- qpdf-doc
- qpid-proton
- qrencode
- qrencode-devel
- qrencode-libs
- qt5-qtcanvas3d
- qt5-qtcanvas3d-examples
- rarian
- rarian-compat
- re2c
- recode
- redhat-lsb
- redhat-lsb-core

- redhat-lsb-cxx
- redhat-lsb-desktop
- redhat-lsb-languages
- redhat-lsb-printing
- redhat-lsb-submod-multimedia
- redhat-lsb-submod-security
- redhat-lsb-supplemental
- redhat-lsb-trialuse
- redhat-menus
- redhat-support-lib-python
- redhat-support-tool
- reflections
- regexp
- relaxngDatatype
- rhsm-gtk
- rpm-plugin-prioreset
- rpmemd
- rsyslog-udpspoof
- ruby-hivex
- ruby-libguestfs
- rubygem-abrt
- rubygem-abrt-doc
- rubygem-bson
- rubygem-bson-doc
- rubygem-bundler-doc
- rubygem-mongo
- rubygem-mongo-doc
- rubygem-net-telnet
- rubygem-xmlrpc

- s390utils-cmsfs
- samba-pidl
- samba-test
- samba-test-libs
- samyak-devanagari-fonts
- samyak-fonts-common
- samyak-gujarati-fonts
- samyak-malayalam-fonts
- samyak-odia-fonts
- samyak-tamil-fonts
- sane-frontends
- sanlk-reset
- sat4j
- scala
- scotch
- scotch-devel
- SDL_sound
- selinux-policy-minimum
- sendmail
- sgabios
- sgabios-bin
- shrinkwrap
- sisu-inject
- sisu-mojos
- sisu-plexus
- skkdic
- SLOF
- smc-anjalioldlipi-fonts
- smc-dyuthi-fonts

- smc-fonts-common
- smc-kalyani-fonts
- smc-raghumalayalam-fonts
- smc-suruma-fonts
- softhsm-devel
- sonatype-oss-parent
- sonatype-plugins-parent
- sos-collector
- sparsehash-devel
- spax
- spec-version-maven-plugin
- spice
- spice-client-win-x64
- spice-client-win-x86
- spice-glib
- spice-glib-devel
- spice-gtk
- spice-gtk-tools
- spice-gtk3
- spice-gtk3-devel
- spice-gtk3-vala
- spice-parent
- spice-protocol
- spice-qxl-wddm-dod
- spice-server
- spice-server-devel
- spice-qxl-xddm
- spice-server
- spice-streaming-agent

- spice-vdagent-win-x64
- spice-vdagent-win-x86
- sssd-libwbclient
- star
- stax-ex
- stax2-api
- stringtemplate
- stringtemplate4
- subscription-manager-initial-setup-addon
- subscription-manager-migration
- subscription-manager-migration-data
- subversion-javahl
- SuperLU
- SuperLU-devel
- supermin-devel
- swig
- swig-doc
- swig-gdb
- swtpm-devel
- swtpm-tools-pkcs11
- system-storage-manager
- tcl-brlapi
- testng
- tibetan-machine-uni-fonts
- timedatex
- tpm-quote-tools
- tpm-tools
- tpm-tools-pkcs11
- treelayout

- trousers
- trousers-lib
- tuned-profiles-compat
- tuned-profiles-nfv-host-bin
- tuned-utils-systemtap
- tycho
- uglify-js
- unbound-devel
- univocity-output-tester
- univocity-parsers
- usbguard-notifier
- usbredir-devel
- utf8cpp
- uthash
- velocity
- vinagre
- vino
- virt-dib
- virt-p2v-maker
- vm-dump-metrics-devel
- weld-parent
- wodim
- woodstox-core
- wqy-microhei-fonts
- wqy-unibit-fonts
- xdelta
- xmlgraphics-commons
- xmlstreambuffer
- xinetd

- xorg-x11-apps
- xorg-x11-drv-qxl
- xorg-x11-server-Xspice
- xpp3
- xsane-gimp
- xsom
- xz-java
- xz-java-javadoc
- yajl-devel
- yp-tools
- ypbind
- ypserv

10.21. 非推奨のデバイスおよび非保守のデバイス

このセクションは、

- RHEL 8 のライフサイクルが終了するまで継続してサポートされるデバイス (ドライバー、アダプター) を説明しますが、本製品の今後のメジャーリリースではサポートされない可能性が高いため、新たに実装することは推奨されません。記載以外のデバイスのサポートは変更しません。これは **非推奨** デバイスです。
- RHEL 8 では入手可能ですが、ルーチンベースでのテストや更新は行われていません。Red Hat は、独自の判断でセキュリティーバグなどの深刻なバグを修正する場合があります。このようなデバイスは実稼働環境では使用しなくなり、次のメジャーリリースでは無効になる可能性が高くなります。これは **未管理** デバイスです。

PCI デバイス ID は、**vendor:device:subvendor:subdevice** の形式です。デバイス ID が記載されていない場合は、対応するドライバーに関連するすべてのデバイスが非推奨になっています。ご使用のシステムでハードウェアの PCI ID を確認するには、**lspci -nn** コマンドを実行します。

表10.1 非推奨のデバイス

デバイス ID	ドライバー	デバイス名
	bnx2	QLogic BCM5706/5708/5709/5716 Driver
	hpsa	Hewlett-Packard Company: Smart アレイコントローラー
0x10df:0x0724	lpfc	Emulex Corporation: OneConnect FCoE Initiator (Skyhawk)

デバイス ID	ドライバー	デバイス名
0x10df:0xe200	lpfc	Emulex Corporation: LPe15000/LPe16000 Series 8Gb/16Gb Fibre Channel Adapter
0x10df:0xf011	lpfc	Emulex Corporation: Saturn: LightPulse Fibre Channel Host Adapter
0x10df:0xf015	lpfc	Emulex Corporation: Saturn: LightPulse Fibre Channel Host Adapter
0x10df:0xf100	lpfc	Emulex Corporation: LPe12000 Series 8Gb Fibre Channel Adapter
0x10df:0xfc40	lpfc	Emulex Corporation: Saturn-X: LightPulse Fibre Channel Host Adapter
0x10df:0xe220	be2net	Emulex Corporation: OneConnect NIC (Lancer)
0x1000:0x005b	megaraid_sas	Broadcom / LSI: MegaRAID SAS 2208 [Thunderbolt]
0x1000:0x006E	mpt3sas	Broadcom / LSI: SAS2308 PCI-Express Fusion-MPT SAS-2
0x1000:0x0080	mpt3sas	Broadcom / LSI: SAS2208 PCI-Express Fusion-MPT SAS-2
0x1000:0x0081	mpt3sas	Broadcom / LSI: SAS2208 PCI-Express Fusion-MPT SAS-2
0x1000:0x0082	mpt3sas	Broadcom / LSI: SAS2208 PCI-Express Fusion-MPT SAS-2
0x1000:0x0083	mpt3sas	Broadcom / LSI: SAS2208 PCI-Express Fusion-MPT SAS-2
0x1000:0x0084	mpt3sas	Broadcom / LSI: SAS2208 PCI-Express Fusion-MPT SAS-2
0x1000:0x0085	mpt3sas	Broadcom / LSI: SAS2208 PCI-Express Fusion-MPT SAS-2
0x1000:0x0086	mpt3sas	Broadcom / LSI: SAS2308 PCI-Express Fusion-MPT SAS-2
0x1000:0x0087	mpt3sas	Broadcom / LSI: SAS2308 PCI-Express Fusion-MPT SAS-2
	myri10ge	Myricom 10G driver (10GbE)
	netxen_nic	QLogic/NetXen (1/10) GbE Intelligent Ethernet Driver

デバイス ID	ドライバー	デバイス名
0x1077:0x2031	qla2xxx	QLogic Corp.: ISP8324-based 16Gb Fibre Channel to PCI Express Adapter
0x1077:0x2532	qla2xxx	QLogic Corp.: ISP2532-based 8Gb Fibre Channel to PCI Express HBA
0x1077:0x8031	qla2xxx	QLogic Corp.: 8300 Series 10GbE Converged Network Adapter (FCoE)
	qla3xxx	QLogic ISP3XXX ネットワークドライバー v2.03.00-k5
0x1924:0x0803	sfc	Solarflare Communications: SFC9020 10G Ethernet Controller
0x1924:0x0813	sfc	Solarflare Communications: SFL9021 10GBASE-T Ethernet Controller
	Soft-RoCE (rdma_rxe)	
	HNS-RoCE	HNS GE/10GE/25GE/50GE/100GE RDMA Network Controller
	liquidio	Cavium LiquidIO Intelligent Server Adapter Driver
	liquidio_vf	Cavium LiquidIO Intelligent Server Adapter Virtual Function Driver

表10.2 未管理デバイス

デバイス ID	ドライバー	デバイス名
	e1000	Intel® PRO/1000 ネットワークドライバー
	mptbase	Fusion MPT SAS ホストドライバー
	mptsas	Fusion MPT SAS ホストドライバー
	mptscsih	Fusion MPT SCSI ホストドライバー
	mptspi	Fusion MPT SAS ホストドライバー

デバイス ID	ドライバー	デバイス名
0x1000:0x0071 [a]	megaraid_sas	Broadcom / LSI: MR SAS HBA 2004
0x1000:0x0073 [a]	megaraid_sas	Broadcom / LSI: MegaRAID SAS 2008 [Falcon]
0x1000:0x0079 [a]	megaraid_sas	Broadcom / LSI: MegaRAID SAS 2108 [Liberator]
	nvmet_tcp	NVMe/TCP ターゲットドライバー
	nvmet-fc	NVMe/Fabrics FC target driver

[a] RHEL 8.0 で無効になり、顧客の要求により RHEL 8.4 で再度有効になりました。

第11章 既知の問題

ここでは、Red Hat Enterprise Linux 8.9 の既知の問題について説明します。

11.1. インストーラーおよびイメージの作成

LPAR およびセキュアブートが有効になっている IBM Power 10 システムでのインストールが失敗します

RHEL インストーラーは、IBM Power 10 システムの静的キーセキュアブートと統合されていません。したがって、セキュアブートオプションを使用して論理パーティション (LPAR) を有効にすると、インストールに失敗し、**Unable to proceed with RHEL-x.x Installation** というエラーが表示されます。

この問題を回避するには、セキュアブートを有効にせずに RHEL をインストールします。システムを起動したら、以下を行います。

1. **dd** コマンドを使用して、署名されたカーネルを PReP パーティションにコピーします。
2. システムを再起動し、セキュアブートを有効にします。

ファームウェアがブートローダーとカーネルを検証すると、システムは正常に起動します。

詳細については、https://www.ibm.com/support/pages/node/6528884 を参照してください。

Bugzilla:2025814[1]

Anaconda がアプリケーションとして実行されているシステムでの予期しない SELinux ポリシー

Anaconda がすでにインストールされているシステムでアプリケーションとして実行されている場合 (たとえば、**–image** anaconda オプションを使用してイメージファイルに別のインストールを実行する場合)、システムはインストール中に SELinux のタイプと属性を変更することを禁止されていません。そのため、SELinux ポリシーの特定の要素は、Anaconda が実行されているシステムで変更される可能性があります。

この問題を回避するには、実稼働システムで Anaconda を実行しないでください。代わりに、一時的な仮想マシンで Anaconda を実行して、実稼働システムの SELinux ポリシーを変更しないようにします。**boot.iso** や **dvd.iso** からのインストールなど、システムインストールプロセスの一部として anaconda を実行しても、この問題の影響は受けません。

Bugzilla:2050140

キックスタートコマンドの auth および authconfig で AppStream リポジトリーが必要になる

インストール中に、キックスタートコマンドの **auth** および **authconfig** で **authselect-compat** パッケージが必要になります。**auth** または **authconfig** を使用したときに、このパッケージがないとインストールに失敗します。ただし、設計上、 **authselect-compat** パッケージは AppStream リポジトリーでしか利用できません。

この問題を回避するには、BaseOS リポジトリーおよび AppStream リポジトリーがインストールプログラムで利用できることを確認するか、インストール中にキックスタートコマンドの **authselect** コマンドを使用します。

Bugzilla:1640697[1]

reboot --kexec コマンドおよび inst.kexec コマンドが、予測可能なシステム状態を提供しない

キックスタートコマンド **reboot --kexec** またはカーネル起動パラメーター **inst.kexec** で RHEL インストールを実行しても、システムの状態が完全な再起動と同じになるわけではありません。これにより、システムを再起動せずにインストール済みのシステムに切り替えると、予期しない結果が発生することがあります。

kexec 機能は非推奨になり、Red Hat Enterprise Linux の今後のリリースで削除されることに注意してください。

Bugzilla:1697896[1]

USB CD-ROM ドライブが Anaconda のインストールソースとして利用できない

USB CD-ROM ドライブがソースで、キックスタート **ignoredisk --only-use=** コマンドを指定すると、インストールに失敗します。この場合、Anaconda はこのソースディスクを見つけ、使用できません。

この問題を回避するには、**harddrive --partition=sdX --dir=**/ コマンドを使用して USB CD-ROM ドライブからインストールします。その結果、インストールは失敗しなくなりました。

Jira:RHEL-4707

インストールプログラムでは、ネットワークアクセスがデフォルトで有効になっていない

一部のインストール機能、たとえば、コンテンツ配信ネットワーク (CDN) を使用したシステムの登録、NTP サーバーサポート、およびネットワークインストールソースなどには、ネットワークアクセスが必要です。ただし、ネットワークアクセスはデフォルトでは有効になっていません。そのためこの機能は、ネットワークアクセスが有効になるまで使用できません。

この問題を回避するには、インストールの開始時にネットワークアクセスを有効にする起動オプション **ip=dhcp** を追加します。オプションで、起動オプションを使用して、ネットワーク上にあるキックスタートファイルまたはリポジトリーを渡しても、問題が解決されます。結果として、ネットワークベースのインストール機能を使用できます。

Bugzilla:1757877[1]

iso9660 ファイルシステムで、ハードドライブがパーティション分割されたインストールが失敗する

ハードドライブが **iso9660** ファイルシステムでパーティションが設定されているシステムには、RHEL をインストールできません。これは、**iso9660** ファイルシステムパーティションを含むハードディスクを無視するように設定されている、更新されたインストールコードが原因です。これは、RHEL が DVD を使用せずにインストールされている場合でも発生します。

この問題を回避するには、インストールの開始前に、キックスタートファイルに次のスクリプトを追加して、ディスクをフォーマットします。

メモ: 回避策を実行する前に、ディスクで利用可能なデータのバックアップを作成します。**wipefs** は、ディスク内の全データをフォーマットします。

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

その結果、インストールでエラーが発生することなく、想定どおりに機能します。

Jira:RHEL-4711

HASH MMU モードの IBM 電源システムが、メモリー割り当ての障害で起動できない

HASH メモリー割り当てユニット (MMU) モードの IBM Power Systems は、最大 192 コアの **kdump** に対応します。そのため、**kdump** が 192 コア以上で有効になっていると、メモリー割り当て失敗が原因でシステムの起動が失敗します。この制限は、**HASH MMU** モードの起動初期段階での RMA メモリーの割り当てによるものです。この問題を回避するには、**kdump** を使用する代わりに、**fadump** を有効にした **Radix MMU** モードを使用します。

Bugzilla:2028361[1]

rpm-ostree ペイロードをインストールすると、RHEL for Edge インストーラーイメージがマウントポイントの作成に失敗する

RHEL for Edge インストーラーイメージなどで使用される **rpm-ostree** ペイロードをデプロイする場合、インストーラーはカスタムパーティションの一部のマウントポイントを適切に作成しません。その結果、インストールは以下のエラーで中止されます。

```
The command 'mount --bind /mnt/sysimage/data /mnt/sysroot/data' exited with the code 32.
```

この問題を回避するには、以下を実行します。

- 自動パーティション設定スキームを使用し、手動でマウントポイントを追加しないでください。
- マウントポイントは、**/var** ディレクトリー内のみに手動で割り当てます。たとえば、**/var/my-mount-point** や、/、**/boot**、**/var** などの標準ディレクトリーです。

その結果、インストールプロセスは正常に終了します。

Jira:RHEL-4744

stig プロファイル修復でビルドされたイメージが FIPS エラーで起動に失敗する

FIPS モードは、RHEL Image Builder ではサポートされていません。**xccdf_org.ssgproject.content_profile_stig** プロファイル修復でカスタマイズされた RHEL Image Builder を使用すると、システムは次のエラーで起動に失敗します。

```
Warning: /boot//.vmlinuz-<kernel version>.x86_64.hmac does not exist
FATAL: FIPS integrity test failed
Refusing to continue
```

/boot ディレクトリーが別のパーティションにあるため、システムイメージのインストール後に **fips-mode-setup --enable** コマンドを使用して FIPS ポリシーを手動で有効にしても機能しません。FIPS が無効になっている場合、システムは正常に起動します。現在、使用可能な回避策はありません。

注記

イメージのインストール後に、**fips-mode-setup --enable** コマンドを使用して、FIPS を手動で有効にすることができます。

Jira:RHEL-4649

11.2. セキュリティー

sshd -T が、暗号、MAC、および KeX アルゴリズムに関する不正確な情報を提供する

sshd -T コマンドの出力には、システム全体の暗号化ポリシー設定や、**/etc/sysconfig/sshd** 内の環境

ファイルから取得でき、**sshd** コマンドの引数として適用されるその他のオプションは含まれていません。これは、アップストリームの OpenSSH プロジェクトが RHEL8 で Red-Hat が提供する暗号化のデフォルトをサポートするための Include ディレクティブをサポートしていなかったために発生します。暗号化ポリシーは、**EnvironmentFile** を使用してサービスを開始するときに、**sshd.service** ユニットの **sshd** 実行可能ファイルにコマンドライン引数として適用されます。この問題を回避するには、**sshd -T $CRYPTO_POLICY** のように、環境ファイルで **source** コマンドを使用し、暗号化ポリシーを引数として **sshd** コマンドに渡します。詳細については、暗号、MAC、または KeX アルゴリズムが **sshd -T** とは異なり、現在の暗号ポリシーレベルで提供されるものとは異なるを参照してください。その結果、**sshd -T** からの出力は、現在設定されている暗号化ポリシーと一致します。

Bugzilla:2044354[1]

インストール中にシステムを強化すると、RHV ハイパーバイザーが正しく動作しないことがある

Red Hat Virtualization Hypervisor (RHV-H) をインストールし、Red Hat Enterprise Linux 8 STIG プロファイルを適用すると、OSCAP Anaconda Add-on が RVH-H ではなく RHEL としてシステムを強化し、RHV-H の必須パッケージを削除する場合があります。その結果、RHV ハイパーバイザーが機能しない場合があります。この問題を回避するには、プロファイルの強化を適用せずに RHV-H システムをインストールし、インストールが完了したら、OpenSCAP を使用してプロファイルを適用します。その結果、RHV ハイパーバイザーは正しく動作します。

Jira:RHEL-1826

CVE OVAL フィードが圧縮形式のみになり、データストリームが SCAP 1.3 標準に準拠していない

Red Hat は、CVE OVAL フィードを bzip2 圧縮形式で提供しています。これらは XML ファイル形式では利用できなくなりました。圧縮されたコンテンツの参照は Security Content Automation Protocol (SCAP) 1.3 仕様で標準化されていないため、サードパーティーの SCAP スキャナーでは、フィードを使用するルールのスキャンで問題が発生する可能性があります。

Bugzilla:2028428

特定の Rsyslog 優先度文字列が正しく機能しない

imtcp に GnuTLS 優先度文字列を設定して、完成していない暗号化をきめ細かく制御できるようになりました。そのため、次の優先度文字列は、Rsyslog リモートログアプリケーションでは正しく機能しません。

```
NONE:+VERS-ALL:-VERS-TLS1.3:+MAC-ALL:+DHE-RSA:+AES-256-GCM:+SIGN-RSA-SHA384:+COMP-ALL:+GROUP-ALL
```

この問題を回避するには、正しく機能する優先度文字列のみを使用します。

```
NONE:+VERS-ALL:-VERS-TLS1.3:+MAC-ALL:+ECDHE-RSA:+AES-128-CBC:+SIGN-RSA-SHA1:+COMP-ALL:+GROUP-ALL
```

したがって、現在の設定は、正しく機能する文字列に限定する必要があります。

Bugzilla:1679512

CIS Server プロファイルを使用すると、Server with GUI および Workstation をインストールできない

CIS Server Level 1 および Level 2 のセキュリティープロファイルは、**Server with GUI** および **Workstation** ソフトウェアの選択と互換性がありません。そのため、**Server with GUI** ソフトウェアの

選択と CIS プロファイルを使用して RHEL 8 をインストールすることはできません。CIS Server Level 1 または Level 2 プロファイルと、これらのソフトウェアの選択のいずれかを使用したインストール試行では、エラーメッセージが生成されます。

> 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.

CIS ベンチマークに従ってシステムを **Server with GUI** または **Workstation** のソフトウェア選択に￥合わせる必要がある場合は、代わりに CIS Workstation Level 1 または Level 2 プロファイルを使用してください。

Bugzilla:1843932

RHEL 8 のキックスタートが、com_redhat_oscap の代わりに org_fedora_oscap を使用

キックスタートは、**com_redhat_oscap** ではなく、**org_fedora_oscap** として Open Security Content Automation Protocol (OSCAP) Anaconda アドオンを参照します。これが、混乱を招く可能性があります。これは、Red Hat Enterprise Linux 7 との互換性を維持するために必要です。

Bugzilla:1665082[1]

libvirt が xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_all_forwarding をオーバーライドする

libvirt 仮想化フレームワークは、**route** または **nat** の転送モードを持つ仮想ネットワークが起動するたびに、IPv4 転送を有効にします。これにより、**xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_all_forwarding** ルールによる設定がオーバーライドされ、後続のコンプライアンススキャンでは、このルールを評価するときに **fail** という結果が報告されます。

この問題を回避するには、次のいずれかのシナリオを適用します。

- シナリオで必要がない場合は、**libvirt** パッケージをアンインストールします。
- **libvirt** によって作成された仮想ネットワークの転送モードを変更します。
- プロファイルを調整して、**xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_all_forwarding** ルールを削除します。

Bugzilla:2118758

fapolicyd ユーティリティーは、変更されたファイルの実行を誤って許可する

正しくは、ファイルの IMA ハッシュはファイルに変更が加えられた後に更新され、**fapolicyd** は変更されたファイルの実行を阻止する必要があります。ただし、IMA ポリシーのセットアップと **evctml** ユーティリティーによるファイルハッシュの違いにより、これは起こりません。その結果、変更されたファイルの拡張属性で IMA ハッシュは更新されません。その結果、**fapolicyd** は、変更されたファイルの実行を誤って許可します。

Jira:RHEL-520[1]

FIPS モードの OpenSSL が、特定の D-H パラメーターのみを受け入れます。

FIPS モードでは、OpenSSL を使用する TLS クライアントは **bad dh value** エラーを返し、手動で生成されたパラメーターを使用するようにサーバーへの TLS 接続を中止します。これは、FIPS 140-2 に準拠するよう設定されている場合、OpenSSL が NIST SP 800-56A rev3 付録 D (RFC 3526 で定義された

グループ 14、15、16、17、18、および RFC 7919 で定義されたグループ) に準拠した Diffie-Hellman パラメーターでのみ機能するためです。また、OpenSSL を使用するサーバーは、その他のパラメーターをすべて無視し、代わりに同様のサイズの既知のパラメーターを選択します。この問題を回避するには、準拠するグループのみを使用します。

Bugzilla:1810911[1]

crypto-policies が Camellia 暗号を誤って許可する。

RHEL 8 システム全体の暗号化ポリシーでは、製品ドキュメントで説明されているように、すべてのポリシーレベルで Camellia 暗号を無効にする必要があります。ただし、Kerberos プロトコルでは、デフォルトでこの Camellia 暗号が有効になります。

この問題を回避するには、**NO-CAMELLIA** サブポリシーを適用します。

```
# update-crypto-policies --set DEFAULT:NO-CAMELLIA
```

これまでに上記のコマンドで、**DEFAULT** から切り替えたことがある場合は、**DEFAULT** を暗号化レベルの名前に置き換えます。

その結果、この回避策を使用して Cemellia 暗号を無効にしている場合に限り、システム全体の暗号化ポリシーを使用する全ポリシーで、この暗号化を適切に拒否できます。

Bugzilla:1919155

OpenSC が CardOS V5.3 カードオブジェクトを正しく検出しない可能性がある

OpenSC ツールキットは、一部の CardOS V5.3 カードで使用されているさまざまな PKCS #15 ファイルオフセットからキャッシュを正しく読み取りません。その結果、OpenSC はカードオブジェクトをリストできず、別のアプリケーションからカードオブジェクトを使用できなくなる可能性があります。

この問題を回避するには、**/etc/opensc.conf** ファイルで **use_file_caching = false** オプションを設定してファイルキャッシュをオフにします。

Jira:RHEL-4077

OpenSC pkcs15-init によるスマートカードのプロビジョニングプロセスが適切に動作しない

file_caching オプションは、デフォルトの OpenSC 設定で有効になっているため、キャッシュ機能は **pkcs15-init** ツールから一部のコマンドを適切に処理しません。したがって、OpenSC を使用したスマートカードのプロビジョニングプロセスは失敗します。

この問題を回避するには、以下のスニペットを **/etc/opensc.conf** ファイルに追加します。

```
app pkcs15-init {
        framework pkcs15 {
                use_file_caching = false;
        }
}
```

pkcs15-init を使用したスマートカードのプロビジョニングは、前述の回避策を適用している場合に限り機能します。

Bugzilla:1947025

SHA-1 署名を使用するサーバーへの接続が GnuTLS で動作しない

証明書の SHA-1 署名は、GuTLS セキュアな通信ライブラリーにより、セキュアでないものとして拒否されます。したがって、TLS のバックエンドとして GnuTLS を使用するアプリケーションは、このような証明書を提供するピアへの TLS 接続を確立することができません。この動作は、その他のシステム暗号化ライブラリーと一貫性がありません。

この問題を回避するには、サーバーをアップグレードして、SHA-256 または強力なハッシュを使用して署名した証明書を使用するか、LEGACY ポリシーに切り替えます。

Bugzilla:1628553[1]

libselinux-python は、そのモジュールからのみ利用可能

libselinux-python パッケージには、SELinux アプリケーション開発用の Python 2 バインディングのみが含まれ、後方互換性に使用されます。このため、**yum install libselinux-python** コマンドを使用すると、デフォルトの RHEL 8 リポジトリーで **libselinux-python** コマンドを利用できなくなりました。

この問題を回避するには、**libselinux-python** モジュールおよび **python27** モジュールの両方を有効にし、以下のコマンドで **libselinux-python** パッケージとその依存関係をインストールします。

```
# yum module enable libselinux-python
# yum install libselinux-python
```

または、1 つのコマンドでインストールプロファイルを使用して **libselinux-python** をインストールします。

```
# yum module install libselinux-python:2.8/common
```

これにより、各モジュールを使用して **libselinux-python** をインストールできます。

Bugzilla:1666328[1]

udica は、--env container=podman で開始したときにのみ UBI 8 コンテナーを処理します。

Red Hat Universal Base Image 8 (UBI 8) コンテナーは、**podman** の値ではなく、**コンテナー** 環境変数を **oci** 値に設定します。これにより、**udica** ツールがコンテナー JavaScript Object Notation (JSON) ファイルを分析しなくなります。

この問題を回避するには、**--env container=podman** パラメーターを指定して、**podman** コマンドで UBI 8 コンテナーを起動します。そのため、**udica** は、上記の回避策を使用している場合に限り、UBI 8 コンテナーの SELinux ポリシーを生成することができます。

Bugzilla:1763210

デフォルトのロギング設定がパフォーマンスに与える悪影響

デフォルトのログ環境設定は、メモリーを 4 GB 以上使用する可能性があり、**rsyslog** で **systemd-journald** を実行している場合は、速度制限値の調整が複雑になります。

詳細は、ナレッジベースの記事 Negative effects of the RHEL default logging setup on performance and their mitigations を参照してください。

Jira:RHELPLAN-10431[1]

/etc/selinux/config の SELINUX=disabled が正常に動作しません。

/etc/selinux/config で **SELINUX=disabled** オプションを使用して SELinux を無効にすると、カーネルが SELinux を有効にして起動し、その後のブートプロセスで無効化モードに切り替わります。これにより、メモリーリークが生じる可能性があります。

この問題を回避するには、SELinux を完全に無効にする必要がある場合に SELinux の使用 の システムの起動時に SELinux モードの変更 で説明されているように、**selinux=0** パラメーターをカーネルコマンドラインに追加して SELinux を無効にすることが推奨されます。

Jira:RHELPLAN-34199[1]

IKE over TCP 接続がカスタム TCP ポートで機能しない

tcp-remoteport Libreswan 設定オプションが適切に動作しません。したがって、デフォルト以外の TCP ポートを指定する必要があるシナリオでは、IKE over TCP 接続を確立することができません。

Bugzilla:1989050

scap-security-guide がアイドルセッションの終了を設定できない

sshd_set_idle_timeout ルールはデータストリームにまだ存在しますが、**sshd** を設定するアイドルセッションタイムアウトの以前の方法は使用できなくなりました。したがって、ルールは **applicable** としてマークされるため、何も強化できません。**systemd** (Logind) など、アイドルセッションの終了を設定する他の方法も使用できません。そのため、**scap-security-guide** は、一定時間が経過した後にアイドルセッションを確実に切断するようにシステムを設定できません。

この問題は、次のいずれかの方法で回避できます。これにより、セキュリティー要件を満たせる可能性があります。

- **accounts_tmout** ルールを設定します。ただし、この変数は **exec** コマンドを使用してオーバーライドできます。
- **configure_tmux_lock_after_time** ルールと **configure_bashrc_exec_tmux** ルールを設定します。これには、**tmux** パッケージをインストールする必要があります。
- 適切な SCAP ルールとともに **systemd** 機能がすでに実装されている RHEL 8.7 以降にアップグレードします。

Jira:RHEL-1804

OSCAP Anaconda アドオンは、グラフィカルインストールで調整されたプロファイルをフェッチしない

OSCAP Anaconda アドオンには、RHEL グラフィカルインストールでセキュリティープロファイルの調整を選択または選択解除するオプションがありません。RHEL 8.8 以降、アドオンはアーカイブまたは RPM パッケージからインストールするときにデフォルトで調整を考慮しません。その結果、インストールでは、OSCAP に合わせたプロファイルを取得する代わりに、次のエラーメッセージが表示されます。

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

この問題を回避するには、キックスタートファイルの **%addon org_fedora_oscap** セクションにパスを指定する必要があります。次に例を示します。

```
xccdf-path = /usr/share/xml/scap/sc_tailoring/ds-combined.xml
tailoring-path = /usr/share/xml/scap/sc_tailoring/tailoring-xccdf.xml
```

その結果、OSCAP 調整プロファイルのグラフィカルインストールは、対応するキックスタート仕様のみで使用できます。

Jira:RHEL-1810

OpenSCAP のメモリー消費の問題

メモリーが限られているシステムでは、OpenSCAP スキャナが途中で停止するか、結果ファイルが生成されない可能性があります。この問題を回避するには、スキャンプロファイルをカスタマイズして、/ ファイルシステム全体の再帰を含むルールの選択を解除します。

- **rpm_verify_hashes**
- **rpm_verify_permissions**
- **rpm_verify_ownership**
- **file_permissions_unauthorized_world_writable**
- **no_files_unowned_by_user**
- **dir_perms_world_writable_system_owned**
- **file_permissions_unauthorized_suid**
- **file_permissions_unauthorized_sgid**
- **file_permissions_ungroupowned**
- **dir_perms_world_writable_sticky_bits**

詳細とその他の回避策については、関連する ナレッジベースの記事 を参照してください。

Bugzilla:2161499

rpm データベースを再構築すると、間違った SELinux ラベルが割り当てられる

rpmdb --rebuilddb コマンドを使用して **rpm** データベースを再構築すると、誤った SELinux ラベルが **rpm** データベースファイルに割り当てられます。その結果、**rpm** データベースを使用する一部のサービスが正しく動作しない可能性があります。データベースの再構築後にこの問題を回避するには、**restorecon -Rv /var/lib/rpm** コマンドを使用してデータベースのラベルを再設定します。

Bugzilla:2166153

Audit 用の ANSSI BP28 HP SCAP ルールが 64 ビット ARM アーキテクチャーで誤って使用される

SCAP セキュリティーガイド (SSG) の ANSSI BP28 High プロファイルには、Linux Audit サブシステムを設定する次の Security Content Automation Protocol (SCAP) ルールが含まれています。しかし、これらのルールは、64 ビット ARM アーキテクチャーでは無効です。

- **audit_rules_unsuccessful_file_modification_creat**
- **audit_rules_unsuccessful_file_modification_open**
- **audit_rules_file_deletion_events_rename**
- **audit_rules_file_deletion_events_rmdir**

- **audit_rules_file_deletion_events_unlink**
- **audit_rules_dac_modification_chmod**
- **audit_rules_dac_modification_chown**
- **audit_rules_dac_modification_lchown**

このプロファイルを使用して 64 ビット ARM マシン上で実行される RHEL システムを設定すると、無効なシステムコールが使用されているため、Audit デーモンが起動しません。

この問題を回避するには、プロファイルの調整を使用して前述のルールをデータストリームから削除するか、**/etc/audit/rules.d** ディレクトリー内のファイルを編集して **-S <syscall>** スニペットを削除します。ファイルに次のシステムコールを含めることはできません。

- creat
- open
- rename
- rmdir
- unlink
- chmod
- chown
- lchown

上記の 2 つの回避策のいずれかを実行すると、64 ビット ARM システムで ANSSI BP28 High プロファイルを使用した後でも、Audit デーモンが起動できるようになります。

Jira:RHEL-1897

キックスタートインストール時のサービス関連のルールの修正が失敗する場合があります。

キックスタートのインストール時に、OpenSCAP ユーティリティーで、サービス **enable** または **disable** 状態の修正が必要でないことが誤って表示されることがあります。これにより、OpenSCAP が、インストール済みシステムのサービスを非準拠状態に設定する可能性があります。回避策として、キックスタートインストール後にシステムをスキャンして修復できます。これにより、サービス関連の問題が修正されます。

Bugzilla:1834716

11.3. サブスクリプションの管理

syspurpose addons が subscription-manager attach --auto 出力に影響しない

Red Hat Enterprise Linux 8 では、**syspurpose** コマンドラインツールの 4 つの属性 (**role**、**usage**、**service_level_agreement**、および **addons**) が追加されました。現在、**role**、**usage**、および **service_level_agreement** のみが、**subscription-manager attach --auto** コマンドの実行の出力に影響します。**addons** 引数に値を設定しても、自動登録されたサブスクリプションには影響がありません。

Bugzilla:1687900

11.4. ソフトウェア管理

cr_compress_file_with_stat() がメモリーリークを引き起こす可能性がある

createrepo_c C ライブラリーには API **cr_compress_file_with_stat()** 関数があります。この関数は、**char **dst** を 2 番目のパラメーターとして宣言します。他のパラメーターによって、**cr_compress_file_with_stat()** は、入力パラメーターとして **dst** を使用するか、割り当てられた文字列を返すために使用します。**dst** の内容をいつ解放するかユーザーに通知しないため、この予測できない動作によりメモリーリークが発生する可能性があります。

この問題を回避するために、**dst** パラメーターを入力としてのみ使用する新しい API **cr_compress_file_with_stat_v2** 関数が追加されました。これは **char *dst** として宣言されます。これにより、メモリーリークが回避されます。

cr_compress_file_with_stat_v2 関数は一時的で、RHEL 8 のみに存在することに注意してください。後で、**cr_compress_file_with_stat()** が代わりに修正されます。

Bugzilla:1973588[1]

スクリプトレットが失敗したときに成功したと報告された YUM トランザクション

RPM バージョン 4.6 以降、インストール後のスクリプトレットは、トランザクションに致命的な影響を与えることなく失敗することが許可されています。この動作は YUM まで伝播します。これにより、スクリプトレットが作成され、パッケージトランザクション全体が成功したと報告されているときに失敗することがあります。

現在利用できる回避策はありません。

これは、RPM と YUM の間で一貫性を保つことが期待される動作であることに注意してください。スクリプトレットの問題は、パッケージレベルで対処する必要があります。

Bugzilla:1986657

11.5. シェルおよびコマンドラインツール

ipmitool は特定のサーバープラットフォームと互換性がありません

ipmitool ユーティリティーは、Intelligent Platform Management Interface (IPMI) をサポートするデバイスの監視、設定、および管理に役立ちます。現在のバージョンの **ipmitool** は、以前の Cipher Suite 3 の代わりに Cipher Suite 17 をデフォルトで使用します。その結果、**ipmitool** は、ネゴシエーション中に Cipher Suite 17 のサポートを発表しましたが、実際にはこの暗号スイートをサポートしていない特定のベアメタルノードとの通信に失敗します。その結果、**ipmitool** は、**no matching cipher suite** エラーメッセージで異常終了します。

詳細は、関連する ナレッジベースの記事 を参照してください。

この問題を解決するには、ベースボード管理コントローラー (BMC) ファームウェアを更新して、Cipher Suite 17 を使用します。

オプションで、BMC ファームウェアの更新が利用できない場合は、**ipmitool** に特定の暗号スイートを強制的に使用させることで、この問題を回避できます。**ipmitool** で管理タスクを呼び出す場合は、使用する暗号スイートの **番号** とともに **ipmitool** コマンドに **-C** オプションを追加します。以下の例を参照してください。

```
# ipmitool -I lanplus -H myserver.example.com -P mypass -C 3 chassis power status
```

Jira:RHEL-6846

復元にクリーンディスクを使用しないと、ReaR がボリュームグループの再作成に失敗する

既存のデータを含むディスクに復元する場合、ReaR は復元の実行に失敗します。

この問題を回避するには、ディスクが以前に使用されていた場合、復元する前にディスクを手動でワイプします。レスキュー環境でディスクをワイプするには、**rear recover** コマンドを実行する前に、次のいずれかのコマンドを使用します。

- ディスクを上書きする **dd** コマンド。
- 使用可能なすべてのメタデータを消去するには、**-a** フラグを指定した **wipefs** コマンド。

/dev/sda ディスクからメタデータをワイプする次の例を参照してください。

```
# wipefs -a /dev/sda[1-9] /dev/sda
```

このコマンドは、最初に **/dev/sda** のパーティションからメタデータをワイプし、次にパーティションテーブル自体をワイプします。

Bugzilla:1925531

coreutils は、誤解を招く EPERM エラーコードを報告することがあります。

statx() システムコールを使用して、GNU コアユーティリティー (**coreutils**) が起動しました。**seccomp** フィルターが、不明なシステムコールに対して EPERM エラーコードを返す場合、EPERM は動作中の **statx()** の syscall が返す実際の **Operation not permitted** エラーと区別できないため、**coreutils** は、誤解を招く EPERM エラーコードを報告します。

この問題を回避するには、**seccomp** フィルターを更新して、**statx()** の syscall を許可するか、不明の syscall の ENOSYS エラーコードを返すようにします。

Bugzilla:2030661

sysstat パッケージの %vmeff メトリックに誤った値が表示される

sysstat パッケージは、ページ再利用効率を測定するための **%vmeff** メトリックを提供します。**sysstat** は、新しいカーネルバージョンで提供されるすべての関連する **/proc/vmstat** 値を解析しないため、**sar -B** コマンドによって返される **%vmeff** 列の値は正しくありません。この問題を回避するには、**/proc/vmstat** ファイルから **%vmeff** 値を手動で計算します。詳細は、Why the **sar(1)** tool reports **%vmeff** values beyond 100 % in RHEL 8 and RHEL 9? を参照してください。

Jira:RHEL-12008

11.6. インフラストラクチャーサービス

FIPS モードの Postfix TLS フィンガープリントアルゴリズムを SHA-256 に変更する必要があります。

RHEL 8 のデフォルトでは、**postfix** は後方互換性に TLS を使用する MD5 フィンガープリントを使用します。ただし、FIPS モードでは、MD5 ハッシュ関数が利用できないため、デフォルトの postfix 設定で TLS が誤って機能する可能性があります。この問題を回避するには、postfix 設定ファイルのハッシュ関数を SHA-256 に変更する必要があります。

詳細は、関連するナレッジベースの記事 Fix postfix TLS in the FIPS mode by switch to SHA-256 instead of the MD5 を参照してください。

Bugzilla:1711885

brltty パッケージは multilib 対応ではない

brltty パッケージの 32 ビット版と 64 ビット版の両方をインストールすることはできません。32 ビット版 (**brltty.i686**) または 64 ビット版 (**brltty.x86_64**) いずれかのパッケージをインストールすることができます。64 ビット版を推奨します。

Bugzilla:2008197

11.7. ネットワーク

ネットワークインターフェイス名の予期しない変更により、RoCE インターフェイスの IP 設定が失われる

RDMA over Converged Ethernet (RoCE) インターフェイスは、次の両方の条件が満たされた場合、ネットワークインターフェイス名の予期しない変更により IP 設定を失います。

- ユーザーが RHEL 8.6 以前のシステムからアップグレードする。
- RoCE カードが UID によって列挙されている。

この問題を回避するには、以下を実行します。

1. 次の内容を含む **/etc/systemd/network/98-rhel87-s390x.link** ファイルを作成します。

```
[Match]
Architecture=s390x
KernelCommandLine=!net.naming-scheme=rhel-8.7

[Link]
NamePolicy=kernel database slot path
AlternativeNamesPolicy=database slot path
MACAddressPolicy=persistent
```

2. システムを再起動して、変更を有効にします。
3. RHEL 8.7 以降にアップグレードします。

機能 ID (FID) によって列挙され、一意ではない RoCE インターフェイスは、**net.naming-scheme=rhel-8.7** カーネルパラメーターを設定しない限り、引き続き予測できないインターフェイス名を使用することに注意してください。この場合、RoCE インターフェイスは **ens** 接頭辞が付いた予測可能な名前に切り替わります。

Jira:RHEL-11398[1]

IPv6_rpfilter オプションが有効になっているシステムでネットワークスループットが低下

firewalld.conf ファイルで **IPv6_rpfilter** オプションが有効になっているシステムでは、100 Gbps リンクなどの高いトラフィックシナリオの場合、現時点でパフォーマンスは最適ではなくネットワークスループットが低下します。この問題を回避するには、**IPv6_rpfilter** オプションを無効にします。これを行うには、**/etc/firewalld/firewalld.conf** ファイルに次の行を追加します。

```
IPv6_rpfilter=no
```

その結果、システムはパフォーマンスが向上しますが、同時にセキュリティーは低下します。

Bugzilla:1871860[1]

11.8. カーネル

カーネル ACPI ドライバーは、PCIe ECAM メモリーリージョンにアクセスできないことを報告します。

ファームウェアが提供する Advanced Configuration and Power Interface (ACPI) テーブルは、PCI バスデバイスの現在のリソース設定 (_CRS) メソッドにおいて PCI バス上のメモリーリージョンを定義しません。したがって、システムの起動時に以下の警告メッセージが表示されます。

```
[    2.817152] acpi PNP0A08:00: [Firmware Bug]: ECAM area [mem 0x30000000-0x31fffffff] not
reserved in ACPI namespace
[    2.827911] acpi PNP0A08:00: ECAM at [mem 0x30000000-0x31fffffff] for [bus 00-1f]
```

ただし、カーネルは依然として **0x30000000-0x31fffffff** メモリーリージョンにアクセスできます。また、そのメモリーリージョンを PCI Enhanced Configuration Access Mechanism (ECAM) に適切に割り当てることができます。以下の出力で 256 バイトオフセットで PCIe 設定領域にアクセスして、PCI ECAM が正常に機能することを確認できます。

```
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
```

これにより、警告メッセージを無視します。

問題の詳細は、Firmware Bug: ECAM area **mem 0x30000000-0x31fffffff** not reserved in ACPI namespace" appears during system boot を参照してください。

Bugzilla:1868526[1]

tuned-adm profile powersave コマンドを使用すると、システムが応答しなくなる

tuned-adm profile powersave コマンドを実行すると、古い Thunderx (CN88xx) プロセッサーを持つ Penguin Valkyrie 2000 2 ソケットシステムが応答しなくなります。これにより、作業を再開するためシステムを再起動することになります。この問題を回避するには、システムが上記の仕様と一致する場合には **powersave** プロファイルの使用を避けてください。

Bugzilla:1609288[1]

HP NMI ウォッチドッグが常にクラッシュダンプを生成しない

特定に場合において、HP NMI ウォッチドッグの **hpwdt** ドライバーは、マスク不可割り込み (NMI) が **perfmon** ドライバーにより使用されたため、HPE ウォッチドッグタイマーが生成した NMI を要求できません。

欠落している NMI は、以下の 2 つの条件のいずれかによって開始されます。

1. Integrated Lights-Out (iLO) サーバー管理ソフトウェアの **NMI 生成** ボタン。このボタンはユーザーがトリガーします。

2. **hpwdt** ウォッチドッグ。デフォルトでは、有効期限により NMI がサーバーに送信されます。

通常、両方のシーケンスは、システムが応答しない場合に発生します。通常、これらの状況の NMI ハンドラーは **kernel panic()** 関数を呼び出します。また、設定されていれば、**kdump** サービスが **vmcore** ファイルを生成します。

ただし、NMI が見つからないため、**kernel panic()** は呼び出されず、**vmcore** が収集されません。

最初のケース (1.) でシステムが応答しない場合は、その状態のままになります。このシナリオを回避するには、仮想 **電源** ボタンを使用してサーバーをリセットするか、電源を切って入れ直します。

2 つ目のケース (2.) では、欠落している NMI が Automated System Recovery (ASR) からのリセットの後 9 秒後に続きます。

HPE Gen9 Server ラインでは、1 桁台の割合でこの問題が発生します。Gen10 の周波数がさらに小さくなる。

Bugzilla:1602962[1]

同一の crash 拡張機能を再読み込みすると、セグメンテーションフォルトが発生する場合がある

読み込み済みのクラッシュ拡張ファイルのコピーを読み込むと、セグメンテーションフォルトが発生する場合があります。現在、crash ユーティリティーは、元のファイルが読み込まれているかどうかを検出します。その結果、crash ユーティリティーに同一のファイルが 2 つ共存するため、名前空間コリジョンが発生し、クラッシュユーティリティーが起動してセグメンテーションフォルトが発生します。

この問題を回避するには、クラッシュ拡張ファイルを一度だけ読み込みます。その結果、セグメンテーションフォルトは上記のシナリオでは発生しなくなりました。

Bugzilla:1906482

仮想マシンへの仮想機能の割り当て時に接続に失敗する

ionic デバイスドライバーを使用する Pensando ネットワークカードは、VLAN タグ設定要求を許可し、ネットワーク仮想機能 (**VF**) を **VM** に割り当てる間にネットワーク接続の設定を試行します。この機能はカードのファームウェアではサポートされていないため、このようなネットワーク接続は失敗します。

Bugzilla:1930576[1]

OPEN MPI ライブラリーは、デフォルトの PML でランタイムが失敗する可能性があります。

OPEN Message Passing Interface (OPEN MPI) 実装 4.0.x シリーズでは、UCX (Unified Communication X) がデフォルトの PPL (ポイントツーポイント) です。OPEN MPI 4.0.x シリーズの新しいバージョンでは、**openib** Byte Transfer Layer (BTL) が非推奨になりました。

ただし、OPEN MPI は **同種** クラスター (同じハードウェアおよびソフトウェア設定) で実行される場合も、UCX は MPI **openlib** の一方向操作に BTL を使用します。これにより、実行エラーが発生する可能性があります。この問題を回避するには、以下を実行します。

- 以下のパラメーターを使用して **mpirun** コマンドを実行します。

```
-mca btl openib -mca pml ucx -x UCX_NET_DEVICES=mlx5_ib0
```

詳細は以下のようになります。

- **-mca btl openib** パラメーターは **openib** BTL を無効にします。
- **-mca pml ucx** パラメーターは、**ucx** PML を使用するように OPEN MPI を設定します。
- **x UCX_NET_DEVICES=** パラメーターは、指定したデバイスを使用するように UCX を制限します。

OPEN MPI は、**異種** クラスター (ハードウェアおよびソフトウェア設定に異なる) を実行する場合は、デフォルトの PML として UCX を使用します。これにより、OPEN MPI ジョブが不安定なパフォーマンス、応答しない動作で実行されたり、またはクラッシュによる不具合とともに実行される可能性があります。この問題を回避するには、UCX の優先度を以下のように設定します。

- 以下のパラメーターを使用して **mpirun** コマンドを実行します。

```
-mca pml_ucx_priority 5
```

これにより、OPEN MPI ライブラリーは、UCX を介して利用可能な別のトランスポート層を選択することができます。

Bugzilla:1866402[1]

vmcore キャプチャーが、メモリーのホットプラグまたはアンプラグの操作を実行した後に失敗する

メモリーのホットプラグまたはホットアンプラグ操作の実行後に、メモリーのレイアウト情報を含むデバイスツリーを更新するとイベントが発生します。これにより、**makedumpfile** ユーティリティーは存在しない物理アドレスにアクセスしようとします。以下の条件を満たすと問題が発生します。

- IBM Power System (little endian) で RHEL 8 を実行する。
- システムで **kdump** サービスまたは **fadump** サービスが有効になっている。

このような場合に、メモリーホットプラグまたはホットアンプラグの操作後にカーネルクラッシュが発生すると、カーネルのキャプチャーで **vmcore** の保存に失敗します。

この問題を回避するには、ホットプラグまたはホットアンプラグ後に **kdump** サービスを再起動します。

```
# systemctl restart kdump.service
```

これにより、上記のシナリオで **vmcore** が正常に保存されます。

Bugzilla:1793389[1]

irqpoll を使用すると vmcore の生成に失敗します。

アマゾンウェブサービス Graviton 1 プロセッサー上で実行される 64 ビット ARM アーキテクチャー上の **nvme** ドライバーの既存の問題により、最初のカーネルに **irqpoll** カーネルコマンドラインパラメーターを指定すると、**vmcore** の生成が失敗します。したがって、カーネルクラッシュ時に **vmcore** が **/var/crash/** ディレクトリーにダンプされません。この問題を回避するには、以下を実行します。

1. **/etc/sysconfig/kdump** ファイルの **KDUMP_COMMANDLINE_REMOVE** 変数に **irqpoll** を追加します。

```
# KDUMP_COMMANDLINE_REMOVE="hugepages hugepagesz slub_debug quiet
log_buf_len swiotlb"
```

2. **/etc/sysconfig/kdump** ファイルの **KDUMP_COMMANDLINE_APPEND** 変数から **irqpoll** を削除します。

```
# KDUMP_COMMANDLINE_APPEND="irqpoll nr_cpus=1 reset_devices
cgroup_disable=memory udev.children-max=2 panic=10 swiotlb=noforce novmcoredd"
```

3. **kdump** サービスを再起動します。

```
# systemctl restart kdump
```

その結果、最初のカーネルが正常に起動し、カーネルクラッシュ時に **vmcore** がキャプチャーされることが予想されます。

Amazon Web Services Graviton 2 および Amazon Web Services Graviton 3 プロセッサーでは、**/etc/sysconfig/kdump** ファイルの **irqpoll** パラメーターを手動で削除する必要がないことに注意してください。

kdump サービスは、大量のクラッシュカーネルメモリーを使用して **vmcore** ファイルをダンプする可能性があります。キャプチャーカーネルには、**kdump** サービス用のメモリーが十分あることを確認します。

この既知の問題の関連情報は、irqpoll カーネルコマンドラインパラメーターにより、vmcore 生成エラーが発生する場合がある を参照してください。

Bugzilla:1654962[1]

コア数が多いシステム上のリアルタイムカーネルのハードウェア認定には、skew-tick=1 ブートパラメーターを渡すことが必要になる場合がある

多数のソケットとコアカウントが大きい大規模なシステムまたは中規模のシステムでは、タイムキーピングシステムで使用される **xtime_lock** のロック競合により、レイテンシーの急増が発生する可能性があります。その結果、レイテンシーの急増およびハードウェア認証のレイテンシーは、マルチプロセッシングシステムで発生する可能性があります。回避策として、**skew_tick=1** ブートパラメーターを追加することで、CPU ごとにタイマーティックをオフセットし、別のタイミングで開始できます。

ロックの競合を回避するには、**skew_tick=1** を有効にします。

1. **grubby** で **skew_tick=1** パラメーターを有効にします。

```
# grubby --update-kernel=ALL --args="skew_tick=1"
```

2. 変更を有効にするために再起動します。

3. ブート中に渡すカーネルパラメーターを表示して、新しい設定を確認します。

```
cat /proc/cmdline
```

skew_tick=1 を有効にすると、消費電力が大幅に増加するため、レイテンシーの影響を受けるリアルタイムワークロードを実行している場合にのみ有効にする必要があります。

Jira:RHEL-9318[1]

RHEL 8 で、デバッグカーネルがクラッシュキャプチャー環境で起動に失敗する

デバッグカーネルはメモリーを大量に消費するので、デバッグカーネルが使用中で、カーネルパニックが発生すると、問題が発生します。その結果、デバッグカーネルはキャプチャーカーネルとして起動できず、代わりにスタックトレースが生成されます。この問題を回避するには、必要に応じてクラッシュカーネルメモリーを増やします。これにより、デバッグカーネルが、クラッシュキャプチャー環境で正常に起動します。

Bugzilla:1659609[1]

起動時にクラッシュカーネルメモリーの割り当てに失敗する

一部の Ampere Altra システムでは、BIOS 設定で 32 ビットリージョンが無効になっていると、起動時にクラッシュカーネルメモリーを割り当てることに失敗します。したがって、**kdump** サービスが起動できません。これは、クラッシュカーネルメモリーを含むのに十分な大きさのフラグメントがない場合に、4 GB 未満のリージョンのメモリーの断片化によって生じます。

この問題を回避するには、以下のように BIOS で 32 ビットのメモリーリージョンを有効にします。

1. システムで BIOS 設定を開きます。
2. **Chipset** メニューを開きます。
3. **Memory Configuration** で、**Slave 32-bit** オプションを有効にします。

これにより、32 ビットリージョン内のクラッシュカーネルメモリー割り当てに成功し、**kdump** サービスが期待どおりに機能します。

Bugzilla:1940674[1]

QAT マネージャーが LKCF のスペアデバイスを残さない

Intel® QuickAssist Technology(QAT) マネージャー (**qatmgr**) はユーザー空間プロセスであり、デフォルトではシステム内のすべての QAT デバイスを使用します。これにより、Linux Kernel Cryptographic Framework(LKCF) には QAT デバイスが残っていません。この動作は予想され、大多数のユーザーはユーザースペースからのアクセラレーションを使用するため、この状況を回避する必要はありません。

Bugzilla:1920086[1]

Solarflare が、最大数の VF(Virtual Function) の作成に失敗する

Solarflare NIC は、リソースが十分にないため、最大数の VF の作成に失敗します。PCIe デバイスが作成できる VF の最大数は、**/sys/bus/pci/devices/PCI_ID/sriov_totalvfs** ファイルで確認できます。この問題を回避するには、起動時に **Solarflare Boot Manager** から、または Solarflare **sfboot** ユーティリティーの使用により、VF の数または VF MSI 割り込みの値を低い値に調整できます。デフォルトの VF MSI 割り込みの値は **8** です。

- **sfboot** を使用して VF MSI 割り込み値を調整するには、以下を実行します。

```
# sfboot vf-msix-limit=2
```

注記

VF MSI 割り込みの値を調整すると、VF のパフォーマンスに影響します。

調整されるパラメーターの詳細は、**Solarflare Server Adapter user guide** を参照してください。

Bugzilla:1971506[1]

page_poison=1 を使用すると、カーネルクラッシュが発生する可能性がある

EFI 実装に問題のあるファームウェアでカーネルパラメーターとして **page_poison=1** を使用すると、オペレーティングシステムが原因でカーネルがクラッシュする可能性があります。デフォルトでは、このオプションは無効になっており、特に実稼働システムでは有効にすることは推奨しません。

Bugzilla:2050411[1]

iwl7260-firmware により、Intel Wi-Fi 6 AX200、AX210、および Lenovo ThinkPad P1 Gen 4 で Wi-Fi が切断される

iwl7260-firmware または **iwl7260-wifi** ドライバーを RHEL 8.7 以降で提供されるバージョンに更新すると、ハードウェアが不正な内部状態になり、その状態を誤って報告します。その結果、Intel Wifi 6 カードが機能せず、次のエラーメッセージが表示される場合があります。

```
kernel: iwlwifi 0000:09:00.0: Failed to start RT ucode: -110
kernel: iwlwifi 0000:09:00.0: WRT: Collecting data: ini trigger 13 fired (delay=0ms)
kernel: iwlwifi 0000:09:00.0: Failed to run INIT ucode: -110
```

未確認の回避策は、システムの電源をオフにしてから再度オンにすることです。再起動しないでください。

Bugzilla:2106341[1]

IBM Power Systems のセキュアブートは移行をサポートしていません

現在、IBM Power Systems では、物理ボリューム (PV) の移行が成功した後、論理パーティション (LPAR) が起動しません。その結果、パーティションでセキュアブートが有効になっているタイプの自動移行は失敗します。

Bugzilla:2126777[1]

kmod の weak-modules がモジュールの相互依存関係で機能しない

kmod パッケージによって提供される **weak-modules** スクリプトは、どのモジュールがインストールされたカーネルと kABI 互換であるかを判別します。ただし、モジュールのカーネル互換性をチェックしている間、**weak-modules は** モジュールシンボルの依存関係を、それらがビルドされたカーネルの上位リリースから下位リリースへと処理します。結果として、異なるカーネルリリースに対して構築された相互依存関係を持つモジュールは互換性がないと解釈される可能性があるため、**weak-modules** はこのシナリオでは機能しません。

この問題を回避するには、新しいカーネルをインストールする前に、最新のストックカーネルに対して追加のモジュールをビルドまたは配置します。

Bugzilla:2103605[1]

Ampere Altra サーバーの kdump が OOM 状態になる

現在、Ampere Altra および Altra Max サーバーのファームウェアが原因で、カーネルが大量のイベント、割り込み、およびコマンドキューを割り当て、メモリーを大量に消費します。その結果、**kdump** カーネルがメモリー不足 (OOM) 状態になります。

この問題を回避するには、**crashkernel=** カーネルオプションの値を 640M に増やして、**kdump** 用に追加のメモリーを予約します。

Bugzilla:2111855[1]

11.9. ファイルシステムおよびストレージ

LUKS ボリュームを格納する LVM mirror デバイスが応答しなくなることがある

セグメントタイプが **mirror** のミラーリング LVM デバイスで LUKS ボリュームを格納すると、特定の条件下で応答しなくなる可能性があります。デバイスが応答しなくなると、すべての I/O 操作を拒否します。

耐障害性のソフトウェア定義ストレージに、LUKS ボリュームをスタックする必要がある場合に、この問題を回避するには、Red Hat は セグメントタイプが **mirror** ではなく **raid1** の LVM RAID 1 デバイスを使用することを推奨します。

raid1 のセグメントタイプは、デフォルトの RAID 設定タイプで、 **mirror** の代わりに、推奨のソリューションとしてこのタイプが使用されます。

mirror デバイスを **raid1** に変換するには、ミラーリングされた LVM デバイスの RAID1 デバイスへの変換 を参照してください。

Bugzilla:1730502[1]

/boot ファイルシステムを LVM に配置することができない

/boot ファイルシステムを LVM 論理ボリュームに配置することはできません。この制限は、以下の理由により存在します。

- EFI システムでは、**EFI システムパーティション** が従来の **/boot** ファイルシステムとして機能します。uEFI 標準では、特定の GPT パーティションタイプと、このパーティションの特定のファイルシステムタイプが必要です。
- RHEL 8 は、システムブートエントリーに **Boot Loader Specification** (BLS) を使用します。この仕様では、プラットフォームのファームウェアが **/boot** ファイルシステムを読み込める必要があります。EFI システムでは、プラットフォームファームウェアは uEFI 標準で定義された **/boot** 設定のみを読み取ることができます。
- GRUB 2 ブートローダーでの LVM 論理ボリュームに対するサポートは完全ではありません。Red Hat は、uEFI や BLS などの標準があるので、この機能のユースケース数が減少しているため、サポートを改善する予定はありません。

Red Hat では、LVM での **/boot** のサポートを提供する予定はありません。代わりに、Red Hat は、**/boot** ファイルシステムを LVM 論理ボリュームに配置する必要がないシステムスナップショットおよびロールバックを管理するツールを提供します。

Bugzilla:1496229[1]

LVM で、複数のブロックサイズを持つボリュームグループが作成できない

vgcreate または **vgextend** などの LVM ユーティリティーでは、物理ボリューム (PV) の論理ブロックサイズが異なるボリュームグループ (VG) を作成できなくなりました。別のブロックサイズの PV で基礎となる論理ボリューム (LV) を拡張するとファイルシステムがマウントに失敗するため、LVM はこの変更を採用しました。

ブロックサイズが混在する VG の作成を再度有効にするには、**lvm.conf** ファイルの **allow_mixed_block_sizes=1** オプションを設定します。

Bugzilla:1768536

LVM writecache の制限

writecache LVM キャッシュメソッドには以下の制限がありますが、**cache** メソッドには存在しません。

- **pvmove** コマンドを使用すると、**writecache** 論理ボリュームに名前を付けることはできません。
- **writecache** を指定した論理ボリュームは、シンプールまたは VDO と組み合わせて使用できません。

以下の制限は、**cache** メソッドにも適用されます。

- **cache** または **writecache** がアタッチされている間は、論理ボリュームのサイズを変更することはできません。

Jira:RHELPLAN-27987[1]、Bugzilla:1808012、Bugzilla:1798631

NVMe/TCP ドライバーを使用する場合、デバイスマッパーマルチパスがサポートされない

NVMe/TCP デバイス上でデバイスマッパーマルチパスを使用すると、パフォーマンスとエラー処理が低下する可能性があります。この問題を回避するには、DM マルチパスツールの代わりにネイティブ NVMe マルチパスを使用します。RHEL 8 の場合、カーネルコマンドラインにオプション **nvme_core.multipath=Y** を追加できます。

Bugzilla:2022359[1]

blk-availability systemd サービスは、複雑なデバイススタックを非アクティブ化する

systemd では、デフォルトのブロック非アクティブ化コードは、仮想ブロックデバイスの複雑なスタックを常に正しく処理するとは限りません。一部の設定では、シャットダウン中に仮想デバイスが削除されない場合があり、エラーメッセージがログに記録されます。この問題を回避するには、次のコマンドを実行して、複雑なブロックデバイススタックを非アクティブ化します。

```
# systemctl enable --now blk-availability.service
```

その結果、複雑な仮想デバイススタックはシャットダウン中に正しく非アクティブ化され、エラーメッセージは生成されません。

Bugzilla:2011699[1]

XFS クォータ警告が頻繁にトリガーされる

クォータタイマーを使用すると、クォータ警告が頻繁にトリガーされるため、ソフトクォータが必要以上に速く実行されます。この問題を回避するには、警告のトリガーを妨げるソフトクォータを使用しないでください。その結果、警告メッセージの量はソフトクォータ制限を強制せず、設定されたタイムアウトを尊重するようになります。

Bugzilla:2059262[1]

11.10. 動的プログラミング言語、WEB サーバー、およびデータベースサーバー

virtualenv ユーティリティーを使用すると Python 3.11 仮想環境の作成が失敗する

python3-virtualenv パッケージによって提供される RHEL 8 の **virtualenv** ユーティリティーは、Python 3.11 と互換性がありません。**virtualenv** を使用して仮想環境を作成しようとすると、次のエラーメッセージが表示されて失敗します。

```
$ virtualenv -p python3.11 venv3.11
Running virtualenv with interpreter /usr/bin/python3.11
ERROR: Virtual environments created by virtualenv < 20 are not compatible with Python 3.11.
ERROR: Use `python3.11 -m venv` instead.
```

Python 3.11 仮想環境を作成するには、代わりに **python3.11 -m venv** コマンドを使用します。このコマンドは、標準ライブラリーの **venv** モジュールを使用します。

Bugzilla:2165702

python3.11-lxml が lxml.isoschematron サブモジュールを提供しない

python3.11-lxml パッケージは、オープンソースライセンスの下にないため、**lxml.isoschematron** サブモジュールなしで配布されます。サブモジュールは ISO Schematron サポートを実装します。代わりに、ISO-Schematron 前の検証を **lxml.etree.Schematron** クラスで利用できます。**python3.11-lxml** パッケージの残りのコンテンツは影響を受けません。

Bugzilla:2157673

MariaDB では PAM プラグインバージョン 1.0 が機能しない

MariaDB 10.3 は、PAM (Pluggable Authentication Modules) プラグインバージョン 1.0 を提供します。**MariaDB 10.5** は、プラグインバージョン 1.0 および 2.0 を提供します。バージョン 2.0 がデフォルトです。

RHEL 8 では、**MariaDB** PAM プラグインバージョン 1.0 は機能しません。この問題を回避するには、**mariadb:10.5** モジュールストリームによって提供される PAM プラグインバージョン 2.0 を使用します。

Bugzilla:1942330

OpenLDAP ライブラリー間のシンボルの競合により、httpd でクラッシュが発生することがある

OpenLDAP が提供する **libldap** ライブラリーと **libldap_r** ライブラリーの両方が、単一のプロセス内にロードされ、使用されると、これらのライブラリー間でシンボルの競合が発生する可能性があります。そのため、**httpd** 設定によって **mod_security** または **mod_auth_openidc** モジュールもロードされると、PHP **ldap** 拡張機能を使用する Apache **httpd** 子プロセスが突然終了する可能性があります。

Apache Portable Runtime (APR) ライブラリーに対する RHEL 8.3 の更新では、**APR_DEEPBIND** 環境変数を設定することでこの問題を回避できます。これにより、**httpd** モジュールのロード時に **RTLD_DEEPBIND** 動的リンカーオプションを使用できるようになります。**APR_DEEPBIND** 環境変数を有効にすると、競合するライブラリーをロードする **httpd** 設定でクラッシュが発生しなくなります。

Bugzilla:1819607[1]

32 ビットアプリケーションで呼び出されると getpwnam() が失敗する場合がある

NIS のユーザーが **getpwnam()** 関数を呼び出す 32 ビットアプリケーションを使用する場合は、**nss_nis.i686** パッケージがないと呼び出しに失敗します。この問題を回避するには、**yum install nss_nis.i686** コマンドを使用して、不足しているパッケージを手動でインストールします。

Bugzilla:1803161

11.11. IDENTITY MANAGEMENT

Samba をプリントサーバーとして実行し、RHEL 8.4 以前から更新する場合にアクションが必要です

今回の更新で、**samba** パッケージが **/var/spool/samba/** ディレクトリーを作成しなくなりました。プリントサーバーとして Samba を使用し、**[printers]** 共有の **/var/spool/samba/** を使用してプリントジョブをスプールすると、SELinux は Samba ユーザーがこのディレクトリーにファイルを作成しないようにします。したがって、印刷ジョブが失敗し、**auditd** サービスは **/var/log/audit/audit.log** に **denied** メッセージを記録します。8.4 以前からシステムを更新した後にこの問題を回避するには、以下を行います。

1. **/etc/samba/smb.conf** ファイルで **[printers]** 共有を探します。
2. 共有定義に **path = /var/spool/samba/** が含まれる場合は、設定を更新して、**path** パラメーターを **/var/tmp/** に設定します。
3. **smbd** サービスを再起動します。

```
# systemctl restart smbd
```

Samba を RHEL 8.5 以降に新しくインストールした場合、アクションは不要です。その場合、**samba-common** パッケージが提供するデフォルトの **/etc/samba/smb.conf** ファイルは、すでに **/var/tmp/** ディレクトリーを使用してプリントジョブをスプールします。

Bugzilla:2009213[1]

--agent-uid pkidbuser オプションを指定して cert-fix ユーティリティーを使用すると、証明書システムが破損します。

--agent-uid pkidbuser オプションを指定して **cert-fix** ユーティリティーを使用すると、証明書システムの LDAP 設定が破損します。したがって、Certificate System は不安定になり、システムの復元に手動の操作が必要になる可能性があります。

Bugzilla:1729215

FIPS モードは、共有シークレットを使用したフォレスト間の信頼を確立することをサポートしません。

NTLMSSP 認証は FIPS に準拠していないため、FIPS モードでフォレスト間の信頼を確立できません。この問題を回避するには、FIPS モードが有効な IdM ドメインと AD ドメインとの間に信頼を確立する際に、Active Directory (AD) 管理アカウントで認証します。

Jira:RHEL-4847

バージョン 1.2.2 へのリベース後の authselect のダウングレードにより、システム認証の破損

authselect パッケージが、最新のアップストリームバージョン **1.2.2** にリベースされました。**authselect** のダウングレードはサポートされておらず、**root** を含むすべてのユーザーに対してシステム認証が破損しています。

authselect パッケージを **1.2.1** 以前にダウングレードした場合は、この問題を回避するために以下の手順を実行します。

1. GRUB ブート画面で、起動するカーネルのバージョンを含む **Red Hat Enterprise Linux** を選択し、**e** を押してエントリーを編集します。

2. **linux** で始まる行の末尾で、**single** を、別の単語で入力し、**Ctrl+X** を押して起動プロセスを開始します。

3. シングルユーザーモードでの起動時に、root パスワードを入力します。

4. 以下のコマンドを使用して authselect 設定を復元します。

```
# authselect select sssd --force
```

Bugzilla:1892761

IdM から AD へのレルム間の TGS 要求が失敗します

IdM Kerberos チケットの 特権属性証明書 (PAC) 情報は、Active Directory (AD) でサポートされていない AES SHA-2 HMAC 暗号化で署名されるようになりました。

その結果、IdM から AD へのレルム間 TGS 要求 (双方向の信頼の設定) は、以下のエラーを出して失敗します。

```
Generic error (see e-text) while getting credentials for <service principal>
```

Jira:RHEL-4910

ldap_id_use_start_tls オプションのデフォルト値を使用する場合の潜在的なリスク

ID ルックアップに TLS を使用せずに **ldap://** を使用すると、攻撃ベクトルのリスクが生じる可能性があります。特に、中間者 (MITM) 攻撃は、攻撃者が、たとえば、LDAP 検索で返されたオブジェクトの UID または GID を変更することによってユーザーになりすますことを可能にする可能性があります。

現在、TLS を強制する SSSD 設定オプション **ldap_id_use_start_tls** は、デフォルトで **false** に設定されています。セットアップが信頼できる環境で動作していることを確認し、**id_provider = ldap** に暗号化されていない通信を使用しても安全かどうかを判断してください。注記: **id_provider = ad** および **id_provider = ipa** は、SASL および GSSAPI によって保護された暗号化接続を使用するため、影響を受けません。

暗号化されていない通信を使用することが安全ではない場合は、**/etc/sssd/sssd.conf** ファイルで **ldap_id_use_start_tls** オプションを **true** に設定して TLS を強制します。デフォルトの動作は、RHEL の将来のリリースで変更される予定です。

Jira:RHELPLAN-155168[1]

RHEL 8.6 から RHEL 8.7 以降への pki-core-debuginfo の更新が失敗する

RHEL 8.6 から RHEL 8.7 以降への **pki-core-debuginfo** パッケージの更新が失敗します。この問題を回避するには、以下のコマンドを実行します。

1. **yum remove pki-core-debuginfo**

2. **yum update -y**

3. **yum install pki-core-debuginfo**

4. **yum install idm-pki-symkey-debuginfo idm-pki-tools-debuginfo**

Jira:RHEL-13125[1]

ドメイン SID の不一致により、移行した IdM ユーザーがログインできない可能性がある

ipa migrate-ds スクリプトを使用して IdM デプロイメントから別のデプロイメントにユーザーを移行する場合、そのユーザーの以前のセキュリティー識別子 (SID) には現在の IdM 環境のドメイン SID がないため、ユーザーが IdM サービスを使用する際に問題が発生する可能性があります。たとえば、これらのユーザーは **kinit** ユーティリティーを使用して Kerberos チケットを取得できますが、ログインできません。この問題を回避するには、ナレッジベースの記事 Migrated IdM users unable to log in due to mismatching domain SIDs を参照してください。

Jira:RHELPLAN-109613[1]

FIPS モードの IdM は、双方向のフォレスト間信頼を確立するための NTLMSSP プロトコルの使用をサポートしない

FIPS モードが有効な Active Directory (AD)と Identity Management (IdM) との間で双方向のフォレスト間の信頼を確立すると、New Technology LAN Manager Security Support Provider (NTLMSSP) 認証が FIPS に準拠していないため、失敗します。FIPS モードの IdM は、認証の試行時に AD ドメインコントローラーが使用する RC4 NTLM ハッシュを受け入れません。

Jira:RHEL-4898

FIPS モードで IdM Vault 暗号化および復号化に失敗する

FIPS モードが有効な場合は、OpenSSL RSA-PKCS1v15 パディング暗号化がブロックされます。その結果、現在は IdM が PKCS1v15 パディングを使用してセッションキーをトランスポート証明書でラップするため、Identity Management (IdM) Vault が正しく機能しません。

Jira:RHEL-12153[1]

Kerberos プリンシパルの有効期限を設定する際の誤った警告

Kerberos プリンシパルのパスワード有効期限を設定すると、32 ビットの符号付き整数変数を使用して、現在のタイムスタンプが有効期限のタイムスタンプと比較されます。有効期限が 68 年以上先の場合、整数変数のオーバーフローが発生し、次の警告メッセージが表示されます。

> Warning: Your password will expire in less than one hour on [expiration date]

このメッセージは無視しても問題ありません。パスワードは設定された日時に正しく期限切れになります。

Bugzilla:2125318

11.12. デスクトップ

ソフトウェアリポジトリーからの flatpak リポジトリーの無効化ができません。

現時点で、GNOME Software ユーティリティーの Software Repositories ツールで **flatpak** リポジトリーを無効化または削除することはできません。

Bugzilla:1668760

Generation 2 の RHEL 8 仮想マシンが Hyper-V Server 2016 ホストで起動できない場合があります。

Microsoft Hyper-V Server 2016 ホストで実行している仮想マシンで RHEL 8 をゲストオペレーティングシステムとして使用すると、仮想マシンが起動しなくなり、GRUB ブートメニューに戻る場合があります。さらに、以下のエラーが Hyper-V イベントログに記録されます。

> The guest operating system reported that it failed with the following error code: 0x1E

このエラーは、Hyper-V ホストの UEFI ファームウェアバグが原因で発生します。この問題を回避するには、Hyper-V Server2019 以降をホストとして使用します。

Bugzilla:1583445[1]

ドラッグアンドドロップが、デスクトップとアプリケーション間で機能しません。

gnome-shell-extensions パッケージのバグにより、ドラッグアンドドロップ機能は現在、デスクトップとアプリケーションの間では機能しません。この機能のサポートは、今後のリリースで追加される予定です。

Bugzilla:1717947

WebKitGTK が IBM Z で Web ページの表示に失敗する

WebKitGTK Web ブラウザーエンジンは、IBM Z アーキテクチャーで Web ページを表示しようとすると失敗します。Web ページは空白のままで、WebKitGTK プロセスが予期せず終了します。

その結果、WebKitGTK を使用して Web ページを表示するアプリケーションの次のような特定の機能を使用できなくなります。

- Evolution メールクライアント
- GNOME オンラインアカウント設定
- GNOME ヘルプアプリケーション

Jira:RHEL-4158

11.13. グラフィックインフラストラクチャー

Radeon ドライバーがハードウェアを正しくリセットできない

現在、**radeon** カーネルドライバーは、**kexec** コンテキストでハードウェアを正しくリセットしません。代わりに **radeon** がフェイルオーバーします。これにより、**kdump** サービスの残りの部分が失敗します。

この問題を回避するには、**/etc/kdump.conf** ファイルに以下の行を追加して、**kdump** で **radeon** を無効にします。

```
dracut_args --omit-drivers "radeon"
force_rebuild 1
```

システムと **kdump** を再起動します。**kdump** の起動後、設定ファイルから **force_rebuild 1** 行が削除される場合があります。

このシナリオでは、ダンププロセス中にグラフィックは利用できませんが、**kdump** は正常に動作します。

Bugzilla:1694705[1]

1 つの MST トポロジーで複数の HDR ディスプレイを使用すると、電源が入らないことがあります。

nouveau ドライバーの NVIDIA Turing GPUs を使用するシステムで、 **DisplayPort** ハブ (ラップトップのドックなど) を使用して HDR プラグインのサポートがあるモニターを複数接続すると、電源が入らないことがあります。これは、全ディスプレイをサポートする帯域幅がハブ上にないと、システムが誤って判断してしまうことが原因で発生します。

Bugzilla:1812577[1]

ビデオメモリーが少なくなったため、ESXi の GUI がクラッシュする可能性がある

vCenter Server 7.0.1 を使用する VMware ESXi 7.0.1 ハイパーバイザーの RHEL 仮想マシンでグラフィカルユーザーインターフェイス (GUI) には、一定量のビデオメモリーが必要です。複数のコンソールまたは高解像度のモニターを仮想マシンに接続する場合、GUI には少なくとも 16 MB のビデオメモリーが必要です。ビデオメモリーが少ないで GUI を起動すると、GUI が突然終了する可能性があります。

この問題を回避するには、仮想マシンに 16 MB 以上のビデオメモリーを割り当てるようにハイパーバイザーを設定します。その結果、仮想マシンの GUI がクラッシュしなくなりました。

この問題が発生した場合は、VMware に報告することを推奨します。

VMware の記事、VMs with high resolution VM console may experience a crash on ESXi 7.0.1 (83194) 、も参照してください。

Bugzilla:1910358[1]

VNC Viewer が、IBM Z で 16 ビットのカラーデプスで誤った色を表示

VNC Viewer アプリケーションは、16 ビットのカラーデプスで IBM Z サーバーの VNC セッションに接続すると、誤った色を表示します。

この問題を回避するには、VNC サーバーで 24 ビットのカラーデプスを設定します。**Xvnc** サーバーの場合は、**Xvnc** 設定で **-depth 16** オプションを **-depth 24** に置き換えます。

その結果、VNC クライアントで色が正しく表示されますが、サーバーでは、より多くのネットワーク帯域幅が使用されます。

Bugzilla:1886147

sudo コマンドを使用してグラフィカルアプリケーションを実行できません。

権限が昇格されたユーザーで、グラフィカルアプリケーションを実行しようとすると、エラーメッセージが表示され、アプリケーションを開くことができません。この障害は、 **Xauthority** ファイルで、通常ユーザーの認証情報を使用して認証するように、**Xwayland** に制限が加えられているため発生します。

この問題を回避するには、**sudo -E** コマンドを使用して、**root** ユーザーとしてグラフィカルアプリケーションを実行します。

Bugzilla:1673073

ARM でハードウェアアクセラレーションがサポートされない

組み込みグラフィックドライバーは、64 ビット ARM アーキテクチャー上のハードウェアアクセラレーションまたは Vulkan API に対応していません。

ARM でハードウェアアクセラレーションまたは Vulkan を有効にするには、プロプライエタリーの Nvidia ドライバーをインストールします。

Jira:RHELPLAN-57914[1]

11.14. RED HAT ENTERPRISE LINUX システムロール

Ansible 2.9 で RHEL システムロールを使用すると、command モジュールで dnf を使用することに関する警告が表示されることがあります。

RHEL 8.8 以降、RHEL システムロールは **dnf** モジュールで **warn** パラメーターを使用しなくなりました。これは、このパラメーターが Ansible Core 2.14 で削除されたためです。ただし、Ansible 2.9 で最新の **rhel-system-roles** パッケージを使用し、ロールがパッケージをインストールすると、次のいずれかの警告が表示される場合があります。

```
[WARNING]: Consider using the dnf module rather than running 'dnf'. If you need to use command
because dnf is insufficient you can add 'warn: false' to
this command task or set 'command_warnings=False' in ansible.cfg to get rid of this message.
```

```
[WARNING]: Consider using the yum, dnf or zypper module rather than running 'rpm'. If you need to
use command because yum, dnf or zypper is insufficient
you can add 'warn: false' to this command task or set 'command_warnings=False' in ansible.cfg to
get rid of this message.
```

これらの警告を非表示にする場合は、**ansible.cfg** ファイルの **[Defaults]** セクションに **command_warnings = False** 設定を追加します。ただし、この設定により Ansible のすべての警告が無効になることに注意してください。

Jira:RHELDOCS-17954

Playbook またはインベントリーでホスト名 localhost を使用して localhost を管理できません

RHEL に **ansible-core 2.13** パッケージが含まれているため、ノードを管理しているのと同じホストで Ansible を実行している場合は、Playbook またはインベントリーで **localhost** ホスト名を使用して実行することはできません。これは、**ansible-core 2.13** が **python38** モジュールを使用し、ライブラリーの多くが欠落しているために発生します。たとえば、**storage** ロールの場合は **blivet**、**network** ロールの場合は **gobject** です。この問題を回避するには、Playbook またはインベントリーでホスト名 **localhost** をすでに使用している場合は、**ansible_connection=local** を使用するか、**ansible_connection=local** オプションを使用して **localhost** をリストするインベントリーファイルを作成することで接続を追加できます。これにより、**localhost** 上のリソースを管理できます。詳細は、RHEL システムロール Playbook を localhost で実行すると失敗する の記事を参照してください。

Bugzilla:2041997

rhc_auth にアクティベーションキーが含まれている場合、rhc システムロールはすでに登録されているシステムで失敗します。

rhc_auth パラメーターにアクティベーションキーが指定されている場合、すでに登録されているシステムで Playbook ファイルを実行すると失敗します。この問題を回避するには、登録済みのシステムで Playbook ファイルを実行するときにアクティベーションキーを指定しないでください。

Bugzilla:2186908

11.15. 仮想化

多数のキューを使用すると、Windows 仮想マシンで障害が発生することがある

仮想 Trusted Platform Module (vTPM) デバイスが有効で、**マルチキュー virtio-net** 機能が 250 を超えるキューを使用するように設定されている場合、Windows 仮想マシン (VM) が失敗することがあります。

この問題は、vTPM デバイスの制限が原因で発生します。vTPM デバイスには、開いているファイル記述子の最大数に関するハードコーディングされた制限があります。新しいキューごとに複数のファイル記述子が開かれるため、内部の vTPM 制限を超えて VM が失敗する可能性があります。

この問題を回避するには、次の 2 つのオプションのいずれかを選択します。

- vTPM デバイスを有効のままにしますが、使用するキューは 250 未満にします。
- 250 を超えるキューを使用するには、vTPM デバイスを無効にします。

Jira:RHEL-13336[1]

Milan 仮想マシンの CPU タイプは、AMD Milan システムで利用できないことがあります。

一部の AMD Milan システムでは、Enhanced REP MOVSB (**erms**) および Fast Short REP MOVSB (**fsrm**) 機能フラグがデフォルトで BIOS で無効になっています。したがって、**Milan** CPU タイプは、これらのシステムで利用できない可能性があります。さらに、機能フラグ設定が異なる Milan ホスト間の仮想マシンのライブマイグレーションが失敗する可能性があります。これらの問題を回避するには、ホストの BIOS で **erms** および **fsrm** を手動で有効にします。

Bugzilla:2077770[1]

AMD EPYC でホストパススルーモードを使用する際に、SMT CPU トポロジーが仮想マシンで検出されない

AMD EPYC ホストで行われた CPU ホストパススルーモードで仮想マシンを起動すると、**TOPOEXT** 機能フラグは存在しません。したがって、仮想マシンは、コアごとに複数のスレッドを持つ仮想 CPU トポロジーを検出できません。この問題を回避するには、ホストパススルーの代わりに EPYC CPU モデルを使用して仮想マシンを起動します。

Bugzilla:1740002

virtio-blk を使用して仮想マシンに LUN デバイスを割り当てると機能しません。

q35 マシンタイプは、移行用の virtio 1.0 デバイスをサポートしないため、RHEL 8 では virtio 1.0 で非推奨となった機能はサポートされません。特に、RHEL 8 ホストで virtio-blk デバイスから SCSI コマンドを送信することはできません。したがって、virtio-blk コントローラーを使用する場合は、物理ディスクを LUN デバイスとして仮想マシンに割り当てると失敗します。

物理ディスクをゲストオペレーティングシステムを通して渡すことは引き続き可能ですが、**device='lun'** オプションではなく、**device='disk'** オプションで設定する必要があることに留意してください。

Bugzilla:1777138[1]

多数の virtio-blk ディスクを使用すると、仮想マシンが起動しないことがある

多数の virtio-blk デバイスを仮想マシンに追加すると、プラットフォームで利用可能な割り込みベクトルの数が使い切られる可能性があります。これが発生すると、仮想マシンのゲスト OS は起動できず、**dracut-initqueue[392]: Warning: Could not boot** エラーが表示されます。

Bugzilla:1719687

iommu_platform=on が IBM POWER で起動に失敗する

RHEL 8 は現在、IBM POWER システムの仮想マシン用の **iommu_platform=on** パラメーターに対応していません。これにより、IBM POWER ハードウェアでこのパラメーターを使用して仮想マシンを起動すると、仮想マシンがシステムの起動プロセス時に応答しなくなります。

Bugzilla:1910848

ibmvfc ドライバーの使用時に IBM POWER ホストが正しく動作するようになりました。

PowerVM 論理パーティション (LPAR) で RHEL 8 を実行すると、**ibmvfc** ドライバーの問題により、さまざまなエラーが発生することがありました。その結果、次のような特定の状況下で、ホスト上でカーネルパニックが発生していました。

- Live Partition Mobility (LPM) 機能の使用
- ホストアダプターのリセット
- SCSI エラー処理機能 (SCSI EH) 機能の使用

この更新により、**ibmvfc** の処理が修正され、前述のカーネルパニックは発生しなくなります。

Bugzilla:1961722[1]

IBM POWER Systems で perf kvm レコード を使用すると、仮想マシンがクラッシュする可能性があります。

IBM POWER ハードウェアのリトルエンディアンバリアントで RHEL 8 ホストを使用する場合は、**perf kvm record** コマンドを使用して KVM 仮想マシンのイベントサンプルを収集すると、仮想マシンが応答しなくなることがあります。この状況は、以下の場合に発生します。

- **perf** ユーティリティーは権限のないユーザーによって使用され、**-p** オプションは仮想マシンを識別するために使用されます (**perf kvm record -e trace_cycles -p 12345**)。
- 仮想マシンが **virsh** シェルを使用して起動している。

この問題を回避するには、**perf kvm** ユーティリティーに **-i** オプションを指定して、**virsh** シェルを使用して作成した仮想マシンを監視します。以下に例を示します。

```
# perf kvm record -e trace_imc/trace_cycles/  -p <guest pid> -i
```

-i オプションを使用する場合、子タスクはカウンターを継承しないため、スレッドは監視されないことに注意してください。

Bugzilla:1924016[1]

特定の CPU モデルの使用時に Hyper-V を有効化した Windows Server 2016 仮想マシンが起動に失敗する

現在、Windows Server 2016 をゲストオペレーティングシステムとして使用し、Hyper-V ロールが有効になっていて、以下の CPU モデルのいずれかを使用する仮想マシンを起動できません。

- EPYC-IBPB
- EPYC

この問題を回避するには、**EPYC-v3** CPU モデルを使用するか、仮想マシンの **xsaves** CPU フラグを手動で有効にします。

Bugzilla:1942888[1]

RHEL 7-ALT ホストから RHEL 8 への POWER9 ゲストの移行に失敗する

現在のリリースでは、RHEL 7-ALT ホストシステムから RHEL 8 に POWER9 仮想マシンを移行すると、**Migration status: active** のステータスで応答がなくなります。

この問題を回避するには、RHEL 7-ALT ホストで Transparent Huge Pages (THP) を無効にすることで、移行が正常に完了します。

Bugzilla:1741436[1]

virt-customize を使用すると、guestfs-firstboot が失敗することがあります。

virt-customize ユーティリティーを使用して仮想マシン (VM) ディスクイメージを変更すると、SELinux パーミッションが正しくないために **guestfs-firstboot** サービスが失敗します。これにより、ユーザーの作成やシステム登録の失敗など、仮想マシンの起動時にさまざまな問題が発生します。

この問題を回避するには、**virt-customize** コマンドに **--selinux-relabel** オプションを指定して使用します。

Bugzilla:1554735

macvtap 仮想ネットワークから正引きインターフェイスを削除すると、このネットワークの接続数がすべてリセットされます。

現在、複数のフォワードインターフェイスを持つ **macvtap** 仮想ネットワークからフォワードインターフェイスを削除すると、ネットワークの他のフォワードインターフェイスの接続ステータスもリセットされます。したがって、ライブネットワーク XML の接続情報が正しくありません。ただし、これは仮想ネットワークの機能に影響を与えるわけではないことに注意してください。この問題を回避するには、ホストで **libvirtd** サービスを再起動します。

Bugzilla:1332758

SLOF が指定された仮想マシンは netcat インターフェイスでの起動に失敗する

netcat(**nc**) インターフェイスを使用して、現在 Slimline Open Firmware(SLOF) プロンプトで待機中の仮想マシンのコンソールにアクセスすると、ユーザー入力は無視され、仮想マシンが応答しないままとなります。この問題を回避するには、仮想マシンに接続する場合は **nc -C** オプションを使用するか、代わりに telnet インターフェイスを使用します。

Bugzilla:1974622[1]

場合によっては、virt-manager で仲介デバイスを仮想マシンに接続すると失敗します

virt-manager アプリケーションは現在、仲介されたデバイスを検出できますが、デバイスがアクティブであるかどうかを認識できません。結果として、**virt-manager** を使用して、非アクティブな仲介デバイスを実行中の仮想マシン (VM) に接続しようとすると失敗します。同様に、非アクティブな仲介デバイスを使用する新しい VM を作成しようとすると、**device not found** エラーで失敗します。

この問題を回避するには、**virt-manager** で使用する前に、**virsh nodedev-start** または **mdevctl start** コマンドを使用して仲介デバイスをアクティブにします。

Bugzilla:2026985

RHEL 9 仮想マシンが POWER8 互換モードでの起動に失敗する

現在、仮想マシン (VM) が次のような CPU 設定も使用している場合、ゲストオペレーティングシステムとして RHEL 9 を実行する仮想マシンの起動は失敗します。

```
<cpu mode="host-model">
  <model>power8</model>
</cpu>
```

この問題を回避するには、RHEL 9 仮想マシンで POWER8 互換モードを使用しないでください。

さらに、POWER8 ホストでは RHEL 9 VM を実行できないことに注意してください。

Bugzilla:2035158

SUID と SGID が virtiofs で自動的にクリアされない

killpriv_v2 機能を使用して **virtiofsd** サービスを実行すると、一部のファイルシステム操作を実行した後、システムが SUID および SGID アクセス許可を自動的にクリアしない場合があります。したがって、アクセス許可をクリアしないと、潜在的なセキュリティー上の脅威が発生する可能性があります。この問題を回避するには、次のコマンドを入力して **killpriv_v2** 機能を無効にします。

```
# virtiofsd -o no_killpriv_v2
```

Bugzilla:1966475[1]

ホストで OVS サービスを再起動すると、実行中の VM でネットワーク接続がブロックされることがある

ホストで Open vSwitch (OVS) サービスが再起動またはクラッシュすると、このホストで実行されている仮想マシン (VM) はネットワークデバイスの状態を回復できません。その結果、仮想マシンがパケットを完全に受信できなくなる可能性があります。

この問題は、**virtio** ネットワークスタックで圧縮された virtqueue 形式を使用するシステムのみに影響します。

この問題を回避するには、**virtio** ネットワークデバイス定義で **packed=off** パラメーターを使用して、圧縮された virtqueue を無効にします。圧縮された virtqueue を無効にすると、状況によっては、ネットワークデバイスの状態を RAM から回復できます。

Bugzilla:1792683

VM 移行中の NFS 障害により、移行が失敗してソース仮想マシンのコアダンプが発生する

現在、仮想マシン (VM) の移行中に NFS サービスまたはサーバーがシャットダウンした場合、ソース VM の QEMU は、実行を再開したときに NFS サーバーに再接続できません。その結果、移行に失敗し、ソース VM でコアダンプが開始されます。現在、使用可能な回避策はありません。

Bugzilla:2177957

nodedev-dumpxml が特定の仲介デバイスの属性を正しく一覧表示しない

現在、**nodedev-dumpxml** は、**nodedev-create** コマンドを使用して作成された仲介デバイスの属性を正しく一覧表示していません。この問題を回避するには、代わりに **nodedev-define** コマンドおよび **nodedev-start** コマンドを使用します。

Bugzilla:2143160

NVIDIA A16 GPU を使用して仮想マシンを起動すると、ホスト GPU が動作を停止する場合がある

現在、NVIDIA A16 GPU パススルーデバイスを使用する仮想マシンを起動すると、ホストシステム上の NVIDIA A16 GPU 物理デバイスが動作を停止する場合があります。

この問題を回避するには、ハイパーバイザーを再起動し、GPU デバイスの **reset_method** を **bus** に設定します。

```
# echo bus > /sys/bus/pci/devices/<DEVICE-PCI-ADDRESS>/reset_method
# cat /sys/bus/pci/devices/<DEVICE-PCI-ADDRESS>/reset_method
bus
```

詳細は、Red Hat ナレッジベースの記事 を参照してください。

Jira:RHEL-2451[1]

11.16. クラウド環境の RHEL

VMware ホストの RHEL 仮想マシンで静的 IP を設定できない

現在、VMware ホストで RHEL を仮想マシンのゲストオペレーティングシステムとして使用すると、DatasourceOVF 機能は正しく機能しません。これにより、**cloud-init** ユーティリティーを使用して、仮想マシンのネットワークを静的 IP に設定し、仮想マシンを再起動すると、仮想マシンのネットワークが DHCP に変更されます。

この問題を回避するには、VMware のナレッジベース を参照してください。

Jira:RHEL-12122

Azure および Hyper-V で kdump が起動しないことがある

Microsoft Azure または Hyper-V ハイパーバイザーでホストされている RHEL 8 ゲストオペレーティングシステムでは、実行後通知が有効な場合に **kdump** カーネルの起動が失敗することがあります。

この問題を回避するには、crash kexec post notifiers を無効にします。

```
# echo N > /sys/module/kernel/parameters/crash_kexec_post_notifiers
```

Bugzilla:1865745[1]

複数のゲストディスクで Hyper-V 仮想マシンを起動する際に、SCSI ホストアドレスが変更することがある

現在、Hyper-V ハイパーバイザーで RHEL 8 仮想マシンを起動すると、場合によっては、**Host, Bus, Target, Lun** (HBTL) SCSI アドレスのホスト部分が変わることがあります。したがって、仮想マシンで HBTL SCSI 識別またはデバイスノードで設定した自動タスクは一貫して動作しません。これは、仮想マシンに複数のディスクがある場合、またはディスクに異なるサイズがある場合に発生します。

この問題を回避するには、以下のいずれかの方法でキックスタートファイルを変更します。

方法 1: SCSI デバイスに永続的な識別子を使用

たとえば、以下の powershell スクリプトを使用すると、特定のデバイス識別子を特定できます。

```
# Output what the /dev/disk/by-id/<value> for the specified hyper-v virtual disk.
# Takes a single parameter which is the virtual disk file.
# Note: kickstart syntax works with and without the /dev/ prefix.
param (
```

```
    [Parameter(Mandatory=$true)][string]$virtualdisk
)

$what = Get-VHD -Path $virtualdisk
$part = $what.DiskIdentifier.ToLower().split('-')

$p = $part[0]
$s0 = $p[6] + $p[7] + $p[4] + $p[5] + $p[2] + $p[3] + $p[0] + $p[1]

$p = $part[1]
$s1 =  $p[2] + $p[3] + $p[0] + $p[1]

[string]::format("/dev/disk/by-id/wwn-0x60022480{0}{1}{2}", $s0, $s1, $part[4])
```

このスクリプトは、ハイパーホストで使用することができます。以下に例を示します。

```
PS C:\Users\Public\Documents\Hyper-V\Virtual hard disks> .\by-id.ps1 .\Testing_8\disk_3_8.vhdx
/dev/disk/by-id/wwn-0x60022480e00bc367d7fd902e8bf0d3b4
PS C:\Users\Public\Documents\Hyper-V\Virtual hard disks> .\by-id.ps1 .\Testing_8\disk_3_9.vhdx
/dev/disk/by-id/wwn-0x600224807270e09717645b1890f8a9a2
```

その後、以下のようにキックスタートファイルでディスクの値を使用できます。

```
part / --fstype=xfs --grow --asprimary --size=8192 --ondisk=/dev/disk/by-id/wwn-
0x600224807270e09717645b1890f8a9a2
part /home --fstype="xfs" --grow --ondisk=/dev/disk/by-id/wwn-
0x60022480e00bc367d7fd902e8bf0d3b4
```

これらの値は仮想ディスクごとに固有であるため、仮想マシンインスタンスごとに設定を行う必要があります。そのため、**%include** 構文を使用して、ディスク情報を別のファイルに配置すると便利です。

方法 2: デバイス選択をサイズで設定

サイズに基づいてディスク選択を設定するキックスタートファイルには、以下のような行を含める必要があります。

```
...

# Disk partitioning information is supplied in a file to kick start
%include /tmp/disks

...

# Partition information is created during install using the %pre section
%pre --interpreter /bin/bash --log /tmp/ks_pre.log

 # Dump whole SCSI/IDE disks out sorted from smallest to largest ouputting
 # just the name
 disks=(`lsblk -n -o NAME -l -b -x SIZE -d -I 8,3`) || exit 1

 # We are assuming we have 3 disks which will be used
 # and we will create some variables to represent
 d0=${disks[0]}
 d1=${disks[1]}
 d2=${disks[2]}
```

```
echo "part /home --fstype="xfs" --ondisk=$d2 --grow" >> /tmp/disks
echo "part swap --fstype="swap" --ondisk=$d0 --size=4096" >> /tmp/disks
echo "part / --fstype="xfs" --ondisk=$d1 --grow" >> /tmp/disks
echo "part /boot --fstype="xfs" --ondisk=$d1 --size=1024" >> /tmp/disks

%end
```

Bugzilla:1906870[1]

cloud-init によってプロビジョニングされ、NFSv3 マウントエントリーで設定された場合、Azure で RHEL インスタンスが起動しない

現在、仮想マシンが **cloud-init** ツールによってプロビジョニングされ、仮想マシンのゲストオペレーティングシステムで **/etc/fstab** ファイルに NFSv3 マウントエントリーがある場合、Microsoft Azure クラウドプラットフォームで RHEL 仮想マシンの起動に失敗します。

Bugzilla:2081114[1]

11.17. サポート性

getattachment コマンドが複数の添付ファイルを一度にダウンロードできない

redhat-support-tool コマンドは、添付ファイルをダウンロードするための **getattachment** サブコマンドを提供します。ただし、**getattachment** は現在、1 つの添付ファイルしかダウンロードできず、複数の添付ファイルをダウンロードできません。

回避策として、**getattachment** サブコマンドで各添付ファイルのケース番号と UUID を渡すことにより、複数の添付ファイルを 1 つずつダウンロードできます。

Bugzilla:2064575

redhat-support-tool が FUTURE 暗号化ポリシーを使用すると機能しない

カスタマーポータル API の証明書が使用する暗号化キーは **FUTURE** のシステム全体の暗号化ポリシーが定義する要件を満たさないので、現時点で **redhat-support-tool** ユーティリティーは、このポリシーレベルでは機能しません。

この問題を回避するには、カスタマーポータル API への接続中に **DEFAULT** 暗号化ポリシーを使用します。

Jira:RHEL-2345

IBM Power Systems (Little Endian) で sos report を実行するとタイムアウトする

数百または数千の CPU を搭載した IBM Power Systems (Little Endian) で **sos report** コマンドを実行すると、**/sys/devices/system/cpu** ディレクトリーの膨大なコンテンツを収集する際のプロセッサープラグインはデフォルトのタイムアウトである 300 秒に達します。回避策として、それに応じてプラグインのタイムアウトを増やします。

- 1 回限りの設定の場合は、次を実行します。

```
# sos report -k processor.timeout=1800
```

- 永続的な変更を行うには、**/etc/sos/sos.conf** ファイルの **[plugin_options]** セクションを編集します。

```
[plugin_options]
# Specify any plugin options and their values here. These options take the form
# plugin_name.option_name = value
#rpm.rpmva = off
processor.timeout = 1800
```

値の例は 1800 に設定されています。特定のタイムアウト値は、特定のシステムに大きく依存します。プラグインのタイムアウトを適切に設定するには、次のコマンドを実行して、タイムアウトなしで 1 つのプラグインを収集するために必要な時間を最初に見積もることができます。

```
# time sos report -o processor -k processor.timeout=0 --batch --build
```

Bugzilla:2011413[1]

11.18. コンテナー

古いコンテナーイメージ内で systemd を実行すると動作しない

古いコンテナーイメージ (例:**centos:7**) で systemd を実行しても動作しません。

```
$ podman run --rm -ti centos:7 /usr/lib/systemd/systemd
 Storing signatures
 Failed to mount cgroup at /sys/fs/cgroup/systemd: Operation not permitted
 [!!!!!!] Failed to mount API filesystems, freezing.
```

この問題を回避するには、以下のコマンドを使用します。

```
# mkdir /sys/fs/cgroup/systemd
# mount none -t cgroup -o none,name=systemd /sys/fs/cgroup/systemd
# podman run --runtime /usr/bin/crun --annotation=run.oci.systemd.force_cgroup_v1=/sys/fs/cgroup -
-rm -ti centos:7 /usr/lib/systemd/systemd
```

Jira:RHELPLAN-96940[1]

第12章 国際化

12.1. RED HAT ENTERPRISE LINUX 8 の多言語

Red Hat Enterprise Linux 8 は、複数の言語のインストールと、要件に応じた言語の変更に対応します。

- 東アジア言語 - 日本語、韓国語、簡体字中国語、および繁体字中国語。
- ヨーロッパ言語 - 英語、ドイツ語、スペイン語、フランス語、イタリア語、ポルトガル語、およびロシア語。

次の表は、さまざまな主要言語に提供されるフォントと入力方法を示しています。

言語	デフォルトフォント (フォントパッケージ)	入力メソッド
英語	dejavu-sans-fonts	
フランス語	dejavu-sans-fonts	
ドイツ語	dejavu-sans-fonts	
イタリア語	dejavu-sans-fonts	
ロシア語	dejavu-sans-fonts	
スペイン語	dejavu-sans-fonts	
ポルトガル語	dejavu-sans-fonts	
簡体字中国語	google-noto-sans-cjk-ttc-fonts、google-noto-serif-cjk-ttc-fonts	ibus-libpinyin、libpinyin
繁体字中国語	google-noto-sans-cjk-ttc-fonts、google-noto-serif-cjk-ttc-fonts	ibus-libzhuyin、libzhuyin
日本語	google-noto-sans-cjk-ttc-fonts、google-noto-serif-cjk-ttc-fonts	ibus-kkc、libkkc
韓国語	google-noto-sans-cjk-ttc-fonts、google-noto-serif-cjk-ttc-fonts	ibus-hangul、libhangul

12.2. RHEL 8 における国際化の主な変更点

RHEL 8 では、RHEL 7 の国際化に以下の変更が加えられています。

- **Unicode 11** コンピューティングの業界標準のサポートが追加されました。

- 国際化は複数のパッケージで配布され、より小さなフットプリントのインストールを可能にします。詳細は、Using langpacks を参照してください。
- 多くの **glibc** ロケールが Unicode Common Locale Data Repository (CLDR) と同期されています。

付録A コンポーネント別のチケットリスト

参考のために、Bugzilla および JIRA チケットのリストをこのドキュメントに記載します。リンクをクリックすると、チケットについて説明したこのドキュメントのリリースノートにアクセスできます。

コンポーネント	チケット
389-ds-base	Bugzilla:2188628、Bugzilla:2166332、Bugzilla:2166284、Bugzilla:2210491、Bugzilla:2220890、Bugzilla:2224505、Bugzilla:1817505
NetworkManager	Bugzilla:2144521、Bugzilla:2151987
リリースノート	Jira:RHELDOCS-16861, Jira:RHELDOCS-16755, Jira:RHELDOCS-16612, Jira:RHELDOCS-17102
SLOF	Bugzilla:1910848
accel-config	Bugzilla:1843266
anaconda	Bugzilla:1770969、Bugzilla:1886985、Bugzilla:1656662、Bugzilla:2050140、Jira:RHEL-4707、Jira:RHEL-4711、Jira:RHEL-4744
ansible-freeipa	Bugzilla:2127901、Bugzilla:2175766、Bugzilla:2127906
apr	Bugzilla:1819607
audit	Bugzilla:2216666
authselect	Bugzilla:1892761
bacula	Jira:RHEL-6859
brltty	Bugzilla:2008197
clevis	Bugzilla:2209058
cloud-init	Bugzilla:2219528、Bugzilla:2230777、Jira:RHEL-12122
cockpit	Bugzilla:1666722
cockpit-appstream	Bugzilla:2212350、Bugzilla:2030836
cockpit-machines	Bugzilla:2173584
coreutils	Bugzilla:2030661
corosync-qdevice	Bugzilla:1784200

コンポーネント	チケット
crash	Bugzilla:1906482
crash-ptdump-command	Bugzilla:1838927
createrepo_c	Bugzilla:1973588
crypto-policies	Bugzilla:2219912、Jira:RHEL-2345、Bugzilla:1919155、Bugzilla:1660839
cups-filters	Bugzilla:2118406
device-mapper-multipath	Bugzilla:2164871、Bugzilla:2022359、Bugzilla:2011699
distribution	Bugzilla:1657927
dnf	Bugzilla:2170093、Bugzilla:1986657
dnf-plugins-core	Bugzilla:2122587、Bugzilla:2092033
edk2	Bugzilla:1741615、Bugzilla:1935497
elfutils	Bugzilla:2182060、Bugzilla:2162495
fapolicyd	Jira:RHEL-628、Jira:RHEL-630、Jira:RHEL-829、Jira:RHEL-520、Bugzilla:2054741
fence-agents	Bugzilla:2187329、Bugzilla:1775847
firewalld	Bugzilla:1871860
fuse	Bugzilla:2171095
gcc	Bugzilla:2168205
gcc-toolset-12-gdb	Bugzilla:2172095
gcc-toolset-13	Bugzilla:2171898
gcc-toolset-13-annobin	Bugzilla:2171923、Bugzilla:2171921
gcc-toolset-13-binutils	Bugzilla:2171924
gcc-toolset-13-gcc	Bugzilla:2172091
gdb	Bugzilla:1853140

コンポーネント	チケット
gfs2-utils	Bugzilla:2180782
glibc	Bugzilla:2180462
gnome-shell-extensions	Bugzilla:1717947
gnome-software	Bugzilla:1668760
gnutls	Bugzilla:2089817、Bugzilla:1628553
golang	Bugzilla:2185260
grafana	Bugzilla:2193250
grafana-pcp	Bugzilla:2193270
grub2	Bugzilla:1583445
grubby	Bugzilla:1900829
initscripts	Bugzilla:1875485
ipa	Bugzilla:2196425, Bugzilla:1821181, Jira:RHEL-4847, Jira:RHEL-4898, Jira:RHEL-12153, Bugzilla:1664719, Bugzilla:1664718, Bugzilla:2101770
ipmitool	Bugzilla:2224567、Jira:RHEL-6846
iproute	Jira:RHEL-424
kernel	Bugzilla:1989283、Bugzilla:2144529、Bugzilla:1753646、Bugzilla:2130727、Bugzilla:1868526、Bugzilla:1694705、Bugzilla:1730502、Bugzilla:1609288、Bugzilla:1602962、Bugzilla:1865745、Bugzilla:1906870、Bugzilla:1924016、Bugzilla:1942888、Bugzilla:1812577、Bugzilla:1910358、Bugzilla:1930576、Bugzilla:1793389、Bugzilla:1654962、Bugzilla:1940674、Bugzilla:1920086、Bugzilla:1971506、Bugzilla:2059262、Bugzilla:2050411、Bugzilla:2106341、Bugzilla:2189645、Bugzilla:1605216、Bugzilla:1519039、Bugzilla:1627455、Bugzilla:1501618、Bugzilla:1633143、Bugzilla:1814836、Bugzilla:1839311、Bugzilla:1696451、Bugzilla:1348508、Bugzilla:1837187、Bugzilla:1660337、Bugzilla:2041686、Bugzilla:1836977、Bugzilla:1878207、Bugzilla:1665295、Bugzilla:1871863、Bugzilla:1569610、Bugzilla:1794513
kernel / Networking / IPSec	Jira:RHEL-1257
kernel / Networking / NIC Drivers	Jira:RHEL-11398

コンポーネント	チケット
kernel / Virtualization / KVM	Jira:RHEL-2451
kernel-rt / Other	Jira:RHEL-9318
kexec-tools	Bugzilla:2173791、Bugzilla:2111855
kmod	Bugzilla:2103605
krb5	Bugzilla:2211390、Jira:RHEL-4910、Bugzilla:2125318、Bugzilla:1877991
leapp-repository	Bugzilla:2097003
libdnf	Bugzilla:2155713
libgnome-keyring	Bugzilla:1607766
libguestfs	Bugzilla:1554735
libnftnl	Bugzilla:2211096
libpfm	Bugzilla:2185653
libreswan	Bugzilla:1989050
libselinux-python-2.8-module	Bugzilla:1666328
libvirt	Bugzilla:1664592、Bugzilla:1332758、Bugzilla:2143160、Bugzilla:1528684
llvm-toolset	Bugzilla:2178806
lvm2	Bugzilla:1496229、Bugzilla:1768536
mariadb	Bugzilla:1942330
mesa	Bugzilla:1886147
nfs-utils	Bugzilla:2081114、Bugzilla:1592011
nftables	Bugzilla:2061942
nodejs	Bugzilla:2186718

コンポーネント	チケット
nss	Bugzilla:1817533、Bugzilla:1645153
nss_nis	Bugzilla:1803161
opencryptoki	Bugzilla:2159697
opencv	Bugzilla:1886310
openmpi	Bugzilla:1866402
opensc	Bugzilla:2097048、Jira:RHEL-4077、Bugzilla:1947025
openscap	Bugzilla:2217441、Bugzilla:2161499
openssh	Bugzilla:2044354
openssl	Bugzilla:1810911
osbuild-composer	Jira:RHEL-4649
oscap-anaconda-addon	Jira:RHEL-1826、Bugzilla:1843932、Bugzilla:1665082、Jira:RHEL-1810
pacemaker	Bugzilla:1876173、Bugzilla:2160206、Bugzilla:2078611、Bugzilla:2030869、Bugzilla:2010084、Bugzilla:1632951、Bugzilla:1578820、Bugzilla:1931023、Bugzilla:2168633
papi	Bugzilla:2111982、Bugzilla:2161146
pcs	Bugzilla:2166294、Bugzilla:2179010、Bugzilla:2189958、Bugzilla:2166289、Bugzilla:1619620、Bugzilla:1851335
perl-HTTP-Tiny	Bugzilla:2228409
pki-core	Bugzilla:1729215、Jira:RHEL-13125、Bugzilla:1628987
podman	Jira:RHELPLAN-154313、Jira:RHELPLAN-154431、Jira:RHELPLAN-154440、Jira:RHELPLAN-154443、Jira:RHELPLAN-163002、Jira:RHELPLAN-160659、Jira:RHELPLAN-154428
postfix	Bugzilla:1787010、Bugzilla:1711885
pykickstart	Bugzilla:1637872
python3.11-lxml	Bugzilla:2157673

コンポーネント	チケット
python36-3.6-module	Bugzilla:2165702
qemu-kvm	Jira:RHEL-13336、Bugzilla:1740002、Bugzilla:1719687、Bugzilla:1966475、Bugzilla:1792683、Bugzilla:2177957、Bugzilla:1651994
rear	Bugzilla:2233526、Bugzilla:1925531、Bugzilla:2083301
redhat-support-tool	Bugzilla:2064575
resource-agents	Bugzilla:2040110、Bugzilla:2049319、Bugzilla:2039692、Bugzilla:2181019
restore	Bugzilla:1997366
rhel-system-roles	Bugzilla:2151371、Bugzilla:2224387、Bugzilla:2190483、Bugzilla:2141961、Bugzilla:2181661、Bugzilla:2211272、Bugzilla:2211723、Bugzilla:2211778、Bugzilla:2216759、Bugzilla:2218204、Bugzilla:2224388、Bugzilla:2218595、Bugzilla:2211273、Bugzilla:2140880、Bugzilla:2192343、Bugzilla:2222809、Jira:RHEL-866、Jira:RHEL-858、Bugzilla:2168738、Bugzilla:2186057、Bugzilla:2209441、Bugzilla:2216521、Bugzilla:2224094、Bugzilla:2224648、Bugzilla:2226077、Bugzilla:2193057、Bugzilla:2222433、Bugzilla:2232391、Bugzilla:2232392、Jira:RHEL-899、Jira:RHEL-907、Jira:RHEL-918、Jira:RHEL-1398、Jira:RHEL-1496、Jira:RHEL-1500、Bugzilla:2186908、Bugzilla:2021685、Bugzilla:2006081
rpm	Bugzilla:1688849
rsyslog	Jira:RHELPLAN-160541、Bugzilla:1679512、Jira:RHELPLAN-10431
rust-toolset	Bugzilla:2191740、Bugzilla:2213875
samba	Bugzilla:2190417、Bugzilla:2009213、Jira:RHELPLAN-13195
scap-security-guide	Bugzilla:2155789, Bugzilla:2157877, Bugzilla:2167999, Bugzilla:2221695, Bugzilla:2129100, Bugzilla:2169857, Bugzilla:2130185, Bugzilla:2175684, Bugzilla:2175882, Bugzilla:2184487, Bugzilla:2192893, Bugzilla:2170530, Bugzilla:2176008, Bugzilla:2209073, Bugzilla:2222583, Bugzilla:2028428, Bugzilla:2118758, Jira:RHEL-1804, Jira:RHEL-1897
selinux-policy	Bugzilla:2172541、Bugzilla:2184348、Bugzilla:2196524、Bugzilla:2166153、Bugzilla:1461914
sos	Bugzilla:2011413
spice	Bugzilla:1849563

コンポーネント	チケット
sssd	Bugzilla:2065692、Bugzilla:2056483、Bugzilla:1947671
subscription-manager	Bugzilla:2170082
sysstat	Jira:RHEL-12008
systemtap	Bugzilla:2186932、Bugzilla:2126805
tang	Bugzilla:2188743
tuned	Bugzilla:2113900
udica	Bugzilla:1763210
udisks2	Bugzilla:2213193
valgrind	Bugzilla:2124345
vdo	Bugzilla:1949163
virt-manager	Bugzilla:2026985
vsftpd	Bugzilla:2069733
wayland	Bugzilla:1673073
webkit2gtk3	Jira:RHEL-4158
which	Bugzilla:2140566
xorg-x11-server	Bugzilla:1698565

コンポーネント	チケット
その他	Jira:RHELDOCS-16405, Bugzilla:2232558, Jira:RHELDOCS-16247, Jira:RHELDOCS-16474, Jira:RHELDOCS-16462, Jira:RHELPLAN-156196, Jira:RHELDOCS-16339, Jira:RHELDOCS-16367, Jira:RHELDOCS-17369, Bugzilla:2236183, Bugzilla:2025814, Bugzilla:2077770, Bugzilla:1777138, Bugzilla:1640697, Bugzilla:1697896, Bugzilla:1961722, Bugzilla:1659609, Bugzilla:1687900, Bugzilla:1757877, Bugzilla:1741436, Jira:RHELPLAN-27987, Jira:RHELPLAN-34199, Jira:RHELPLAN-57914, Jira:RHELPLAN-96940, Bugzilla:1974622, Bugzilla:2028361, Bugzilla:2041997, Bugzilla:2035158, Jira:RHELPLAN-109613, Bugzilla:2126777, Bugzilla:1690207, Bugzilla:1559616, Bugzilla:1889737, Bugzilla:1906489, Bugzilla:1769727, Jira:RHELPLAN-27394, Jira:RHELPLAN-27737, Jira:RHELDOCS-16861, Bugzilla:1642765, Bugzilla:1646541, Bugzilla:1647725, Jira:RHELDOCS-17380, Bugzilla:1932222, Bugzilla:1686057, Bugzilla:1748980, Jira:RHELPLAN-71200, Jira:RHELPLAN-45858, Bugzilla:1871025, Bugzilla:1871953, Bugzilla:1874892, Bugzilla:1916296, Jira:RHELPLAN-100400, Bugzilla:1926114, Bugzilla:1904251, Bugzilla:2011208, Jira:RHELPLAN-59825, Bugzilla:1920624, Jira:RHELPLAN-70700, Bugzilla:1929173, Jira:RHELPLAN-85066, Jira:RHELPLAN-98983, Bugzilla:2009113, Bugzilla:1958250, Bugzilla:2038929, Bugzilla:2006665, Bugzilla:2029338, Bugzilla:2061288, Bugzilla:2060759, Bugzilla:2055826, Bugzilla:2059626, Jira:RHELPLAN-133171, Bugzilla:2142499, Jira:RHELDOCS-16755, Jira:RHELPLAN-146398, Jira:RHELPLAN-153267, Bugzilla:2225332, Jira:RHELPLAN-147538, Jira:RHELDOCS-16612, Jira:RHELDOCS-17102, Jira:RHELDOCS-16300

付録B 改訂履歴

0.0-12

2024 年 6 月 7 日 (金)、Brian Angelica (bangelic@redhat.com)

- Jira:RHELDOCS-17954 の既知の問題を更新しました (Red Hat Enterprise Linux システムロール)。

0.0-11

2024 年 5 月 10 日 (金) Brian Angelica (bangelic@redhat.com)

- BZ#1690207 でテクニカルプレビューを更新。

0.0-10

2024 年 5 月 9 日 (木)、Gabriela Fialova (gfialova@redhat.com)

- 既知の問題 BZ#1730502 (ストレージ) を更新。

0.0-9

2024 年 4 月 29 日 (月)、Gabriela Fialova (gfialova@redhat.com)

- BZ#2093355 (セキュリティー) の機能拡張を追加しました。

0.0-8

2024 年 3 月 4 日 (月)、Lucie Vařáková (lvarakova@redhat.com)

- バグ修正 Jira:SSSD-6096 (アイデンティティー管理) を追加しました

0.0-7

2024 年 2 月 29 日 (木)、Lucie Vařáková (lvarakova@redhat.com)

- 非推奨の機能 Jira:RHELDOCS-17641 (ネットワーク) を追加しました。

0.0-6

2024 年 2 月 13 日火曜日、Lucie Vařáková (lvarakova@redhat.com)

- 非推奨の機能 Jira:RHELDOCS-17573 (アイデンティティー管理) を追加しました。

0.0-5

2024 年 2 月 2 日 (金)、Lucie Vařáková (lvarakova@redhat.com)

- 既知の問題 BZ#1834716 (セキュリティー) を追加しました。
- Jira:RHELDOCS-16755 非推奨機能に関する注記 (コンテナー) を更新しました。

0.0-4

2024 年 1 月 19 日 (金)、Lucie Vařáková (lvarakova@redhat.com)

- Python Jira:RHELDOCS-17369 (動的プログラミング言語、Web およびデータベースサーバー) に関連する機能拡張を追加しました。
- 拡張機能 Jira:RHELDOCS-16367 (Web コンソール) を追加しました。

0.0-3

2024 年 1 月 10 日 (水)、Lucie Vařáková (lvarakova@redhat.com)

- リベース BZ#2196425 (アイデンティティー管理) を追加しました。
- Jira:RHELPLAN-156196 の新機能の説明 (サポート可能性) を更新しました。
- 非推奨の機能 Jira:RHELDOCS-17380 (セキュリティー) を追加しました。
- その他の若干の更新

0.0-2

2023 年 11 月 16 日 (木) Lenka Špačková (lspackova@redhat.com)

- **Node.js 20** が完全にサポートされるようになりました (BZ#2186718)。

0.0-1

2023 年 11 月 15 日 (水)、Lucie Vařáková (lvarakova@redhat.com)

- Red Hat Enterprise Linux 8.9 リリースノートのリリース。

0.0-0

2023 年 9 月 27 日 (水)、Lucie Vařáková (lvarakova@redhat.com)

- Red Hat Enterprise Linux 8.9 ベータ版リリースノートのリリース。